REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT

Bid Reference No.: BAC4G&S-2018-002

Approved Budget for the Contract: PhP512,000,000.00

**DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY
BIDS AND AWARDS COMMITTEE FOR GOODS AND SERVICES**

MAY 2018

TABLE OF CONTENTS

Section I.
Invitation to Bid

REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

INVITATION TO BID

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT

Bid Reference No. BAC4G&S-2018-002

Approved Budget for the Contract: PhP512,000,000.00

1. The **DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT),** through the 2018 General Appropriations Act, intends to apply the sum of **Five Hundred Twelve Million Pesos (PhP512,000,000.00),** being the Approved Budget for the Contract (ABC) for the **SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT.**

Description	Qty	Total ABC (PhP) (VAT Inclusive)	Cost/Price of Bid Documents (cash Payment only) (PhP)
Supply, Installation and Delivery of Cybersecurity Management System Project	1 Lot	512,000,000.00	75,000.00

2. Bids exceeding the stated amount of ABC shall automatically be rejected at the bid opening. Late bids shall not be accepted.

3. Delivery Place and Delivery Period:

Delivery Place	Delivery Period
Department of Information and Communications Technology (DICT), 49 Don A. Roces Ave, Quezon City	Within ten (10) months days from receipt of Notice to Proceed

4. A prospective Bidder should have completed within the last five (5) years from the date of submission and receipt of bids at least one (1) single contract of similar nature amounting to at least fifty percent (50%) of the ABC.

   For this project, "similar in nature" shall mean "Security Operations Center (SOC)".

5. Bidding will be conducted through open competitive bidding procedures using a non-discretionary "pass/fail" criterion as specified in the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (RA) 9184, otherwise known as the "Government Procurement Reform Act".
6. Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA 5183.

7. The Invitation to Bid and Bidding Documents may be downloaded from the website of the Philippine Government Electronic Procurement System (PhilGEPS) and DICT website (dict.gov.ph).

8. The complete set of Bidding Documents may be acquired by interested bidders upon payment of a nonrefundable fee as indicated above. The Bidding Documents shall be received personally by the prospective Bidder or his duly authorized representative upon presentation of proper document.

9. The Schedule of Bidding Activities shall be as follows:

ACTIVITIES	TIME	VENUE
Sale and Issuance of Bid Documents	From 28 May 2018, 9AM to 25 June 2018, 12 Noon	Bids and Awards Committee Office, Lower Ground Floor, DICT Office, C.P. Garcia Avenue, Diliman, Q.C.
Pre-Bid Conference	7 June 2018 1:30 PM	Executive Lounge, DICT Building, C.P. Garcia Avenue, Diliman, Q.C.
Submission of Bids	25 June 2018 12 Noon	Lobby, DICT Building, C.P. Garcia Avenue, Diliman, Q.C.
Opening of Bids	25 June 2018 1:30 PM	Executive Lounge, DICT Building, C.P. Garcia Avenue, Diliman, Q.C.

10. For the Pre-Bid Conference, bidders are encouraged to send their authorized technical representatives or personnel who are familiar with the bid requirements and will prepare the documents for the bidder.

11. DICT reserves the right to waive any formality in the responses to the eligibility requirements and to this invitation. DICT further reserves the right to accept or reject any Bid, to annul the bidding process, and to reject all Bids at any time prior to contract award, and makes no assurance that contract shall be entered into as a result of this invitation, without thereby incurring any liability to the affected Bidder/s.

12. For further information, please refer to:
Engr. Thelma D. Villamorel
Head BAC Secretariat
Department of Information and Communications Technology
C.P. Garcia Avenue, Diliman, Quezon City
Telephone No.: 920-0101 local 1831
Email Address: bac4g&s@dict.gov.ph
Website: www.dict.gov.ph

JOHN HENRY D. NAGA
Vice Chairperson, BAC4G&S

Section II.
Instruction to Bidders

A. General

1. Scope of Bid

1.1. The Procuring Entity named in the **BDS** invites bids for the supply and delivery of the Goods as described in Section VII. Technical Specifications.

1.2. The name, identification, and number of lots specific to this bidding are provided in the **BDS**. The contracting strategy and basis of evaluation of lots is described in **ITB** Clause 28.

2. Source of Funds

The Procuring Entity has a budget or has received funds from the Funding Source named in the **BDS**, and in the amount indicated in the **BDS**. It intends to apply part of the funds received for the Project, as defined in the **BDS**, to cover eligible payments under the contract.

3. Corrupt, Fraudulent, Collusive, and Coercive Practices

3.1. Unless otherwise specified in the **BDS**, the Procuring Entity as well as the bidders and suppliers shall observe the highest standard of ethics during the procurement and execution of the contract. In pursuance of this policy, the Procuring Entity:

(a) defines, for purposes of this provision, the terms set forth below as follows:

(i) "corrupt practice" means behavior on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves, others, or induce others to do so, by misusing the position in which they are placed, and includes the offering, giving, receiving, or soliciting of anything of value to influence the action of any such official in the procurement process or in contract execution; entering, on behalf of the government, into any contract or transaction manifestly and grossly disadvantageous to the same, whether or not the public officer profited or will profit thereby, and similar acts as provided in RA 3019.

(ii) "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Procuring Entity, and includes collusive practices among Bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the Procuring Entity of the benefits of free and open competition.

(iii) "collusive practices" means a scheme or arrangement between two or more Bidders, with or without the knowledge of the Procuring Entity, designed to establish bid prices at artificial, non-competitive levels.

(iv) "coercive practices" means harming or threatening to harm, directly or indirectly, persons, or their property to influence their participation in a procurement process, or affect the execution of a contract;

(v) "obstructive practice" is

(aa) deliberately destroying, falsifying, altering or concealing of evidence material to an administrative proceedings or investigation or making false statements to investigators in order to materially impede an administrative proceedings or investigation of the Procuring Entity or any foreign government/foreign or international financing institution into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the administrative proceedings or investigation or from pursuing such proceedings or investigation; or

(bb) acts intended to materially impede the exercise of the inspection and audit rights of the Procuring Entity or any foreign government/foreign or international financing institution herein.

(b) will reject a proposal for award if it determines that the Bidder recommended for award has engaged in any of the practices mentioned in this Clause for purposes of competing for the contract.

3.2. Further, the Procuring Entity will seek to impose the maximum civil, administrative, and/or criminal penalties available under applicable laws on individuals and organizations deemed to be involved in any of the practices mentioned in **ITB** Clause 3.1(a).

3.3. Furthermore, the Funding Source and the Procuring Entity reserve the right to inspect and audit records and accounts of a bidder or supplier in the bidding for and performance of a contract themselves or through independent auditors as reflected in the **GCC** Clause 3.

4. Conflict of Interest

4.1. All Bidders found to have conflicting interests shall be disqualified to participate in the procurement at hand, without prejudice to the imposition of appropriate administrative, civil, and criminal sanctions. A Bidder may be considered to have conflicting interests with another Bidder in any of the events described in paragraphs (a) through (c) below and a general conflict of interest in any of the circumstances set out in paragraphs (d) through (g) below:

(a) A Bidder has controlling shareholders in common with another Bidder;

(b) A Bidder receives or has received any direct or indirect subsidy from any other Bidder;

(c) A Bidder has the same legal representative as that of another Bidder for purposes of this bid;

(d) A Bidder has a relationship, directly or through third parties, that puts them in a position to have access to information about or influence on the bid of another Bidder or influence the decisions of the Procuring Entity regarding this bidding process;

(e) A Bidder submits more than one bid in this bidding process. However, this does not limit the participation of subcontractors in more than one bid;

(f) A Bidder who participated as a consultant in the preparation of the design or technical specifications of the Goods and related services that are the subject of the bid; or

(g) A Bidder who lends, or temporarily seconds, its personnel to firms or organizations which are engaged in consulting services for the preparation related to procurement for or implementation of the project, if the personnel would be involved in any capacity on the same project.

4.2. In accordance with Section 47 of the IRR of RA 9184, all Bidding Documents shall be accompanied by a sworn affidavit of the Bidder that it is not related to the Head of the Procuring Entity (HoPE), members of the Bids and Awards Committee (BAC), members of the Technical Working Group (TWG), members of the BAC Secretariat, the head of the Project Management Office (PMO) or the end-user unit, and the project consultants, by consanguinity or affinity up to the third civil degree. On the part of the Bidder, this Clause shall apply to the following persons:

(a) If the Bidder is an individual or a sole proprietorship, to the Bidder himself;

(b) If the Bidder is a partnership, to all its officers and members;

(c) If the Bidder is a corporation, to all its officers, directors, and controlling stockholders;

(d) If the Bidder is a cooperative, to all its officers, directors, and controlling shareholders or members; and

(e) If the Bidder is a joint venture (JV), the provisions of items (a), (b), (c), or (d) of this Clause shall correspondingly apply to each of the members of the said JV, as may be appropriate.

Relationship of the nature described above or failure to comply with this Clause will result in the automatic disqualification of a Bidder.

5. Eligible Bidders

5.1. Unless otherwise provided in the **BDS**, the following persons shall be eligible to participate in this bidding:

(a) Duly licensed Filipino citizens/sole proprietorships;

(b) Partnerships duly organized under the laws of the Philippines and of which at least sixty percent (60%) of the interest belongs to citizens of the Philippines;

(c) Corporations duly organized under the laws of the Philippines, and of which at least sixty percent (60%) of the outstanding capital stock belongs to citizens of the Philippines;

(d) Cooperatives duly organized under the laws of the Philippines; and

(e) Persons/entities forming themselves into a Joint Venture (JV), *i.e.*, a group of two (2) or more persons/entities that intend to be jointly and severally responsible or liable for a particular contract: Provided, however, that Filipino ownership or interest of the JV concerned shall be at least sixty percent (60%).

5.2. Foreign bidders may be eligible to participate when any of the following circumstances exist, as specified in the **BDS**:

(a) When a Treaty or International or Executive Agreement as provided in Section 4 of RA 9184 and its IRR allow foreign bidders to participate;

(b) Citizens, corporations, or associations of a country, the laws or regulations of which grant reciprocal rights or privileges to citizens, corporations, or associations of the Philippines;

(c) When the Goods sought to be procured are not available from local suppliers; or

(d) When there is a need to prevent situations that defeat competition or restrain trade.

5.3. Government owned or –controlled corporations (GOCCs) may be eligible to participate only if they can establish that they (a) are legally and financially autonomous, (b) operate under commercial law, and (c) are not attached agencies of the Procuring Entity.

5.4. Unless otherwise provided in the **BDS**, the Bidder must have completed a Single Largest Completed Contract (SLCC) similar to the Project and the value of which, adjusted, if necessary, by the Bidder to current prices using the Philippine Statistics Authority (PSA) consumer price index, must be at least equivalent to a percentage of the ABC stated in the **BDS**.

For this purpose, contracts similar to the Project shall be those described in the **BDS**, and completed within the relevant period stated in the Invitation to Bid and **ITB** Clause 12.1(a)(ii).

5.5. The Bidder must submit a computation of its Net Financial Contracting Capacity (NFCC), which must be at least equal to the ABC to be bid, calculated as follows:

NFCC = [(Current assets minus current liabilities) (15)] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started, coinciding with the contract to be bid.

The values of the domestic bidder's current assets and current liabilities shall be based on the latest Audited Financial Statements submitted to the BIR.

For purposes of computing the foreign bidders' NFCC, the value of the current assets and current liabilities shall be based on their audited financial statements prepared in accordance with international financial reporting standards.

If the prospective bidder opts to submit a committed Line of Credit, it must be at least equal to ten percent (10%) of the ABC to be bid. If issued by a foreign universal or commercial bank, it shall be confirmed or authenticated by a local universal or commercial bank.

6. Bidder's Responsibilities

6.1. The Bidder or its duly authorized representative shall submit a sworn statement in the form prescribed in Section VIII. Bidding Forms as required in **ITB** Clause 12.1(b)(iii).

6.2. The Bidder is responsible for the following:

(a) Having taken steps to carefully examine all of the Bidding Documents;

(b) Having acknowledged all conditions, local or otherwise, affecting the implementation of the contract;

(c) Having made an estimate of the facilities available and needed for the contract to be bid, if any;

(d) Having complied with its responsibility to inquire or secure Supplemental/Bid Bulletin(s) as provided under **ITB** Clause 10.4.

(e) Ensuring that it is not "blacklisted" or barred from bidding by the GOP or any of its agencies, offices, corporations, or LGUs, including foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the GPPB;

(f) Ensuring that each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

(g) Authorizing the HoPE or its duly authorized representative/s to verify all the documents submitted;

(h) Ensuring that the signatory is the duly authorized representative of the Bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the Bidder in the bidding, with the duly notarized Secretary's Certificate attesting to such fact, if the Bidder is a corporation, partnership, cooperative, or joint venture;

(i) Complying with the disclosure provision under Section 47 of RA 9184 and its IRR in relation to other provisions of RA 3019;

(j) Complying with existing labor laws and standards, in the case of procurement of services; Moreover, bidder undertakes to:

(i) Ensure the entitlement of workers to wages, hours of work, safety and health and other prevailing conditions of work as established by national laws, rules and regulations; or collective bargaining agreement; or arbitration award, if and when applicable.

In case there is a finding by the Procuring Entity or the DOLE of underpayment or non-payment of workers' wage and wage-related benefits, bidder agrees that the performance security or portion of the contract amount shall be withheld in favor of the complaining workers pursuant to appropriate provisions of Republic Act No. 9184 without prejudice to the institution of appropriate actions under the Labor Code, as amended, and other social legislations.

(ii) Comply with occupational safety and health standards and to correct deficiencies, if any.

In case of imminent danger, injury or death of the worker, bidder undertakes to suspend contract implementation pending clearance to proceed from the DOLE Regional Office and to comply with Work Stoppage Order; and

(iii) Inform the workers of their conditions of work, labor clauses under the contract specifying wages, hours of work and other benefits under prevailing national laws, rules and regulations; or collective bargaining agreement; or arbitration award, if and when applicable, through posting in two (2) conspicuous places in the establishment's premises; and

(k) Ensuring that it did not give or pay, directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

Failure to observe any of the above responsibilities shall be at the risk of the Bidder concerned.

6.3. The Bidder is expected to examine all instructions, forms, terms, and specifications in the Bidding Documents.

6.4. It shall be the sole responsibility of the Bidder to determine and to satisfy itself by such means as it considers necessary or desirable as to all matters pertaining to the contract to be bid, including: (a) the location and the nature of this Project; (b) climatic conditions; (c) transportation facilities; and (d) other factors that may affect the cost, duration, and execution or implementation of this Project.

6.5. The Procuring Entity shall not assume any responsibility regarding erroneous interpretations or conclusions by the prospective or eligible bidder out of the data furnished by the procuring entity. However, the Procuring Entity shall ensure that all information in the Bidding Documents, including bid/supplemental bid bulletin/s issued, are correct and consistent.

6.6. Before submitting their bids, the Bidder is deemed to have become familiar with all existing laws, decrees, ordinances, acts and regulations of the Philippines which may affect this Project in any way.

6.7. The Bidder shall bear all costs associated with the preparation and submission of his bid, and the Procuring Entity will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

6.8. The Bidder should note that the Procuring Entity will accept bids only from those that have paid the applicable fee for the Bidding Documents at the office indicated in the Invitation to Bid.

7. Origin of Goods

Unless otherwise indicated in the **BDS**, there is no restriction on the origin of goods other than those prohibited by a decision of the United Nations Security Council taken under Chapter VII of the Charter of the United Nations, subject to **ITB** Clause 27.1.

8. Subcontracts

8.1. Unless otherwise specified in the **BDS**, the Bidder may subcontract portions of the Goods to an extent as may be approved by the Procuring Entity and stated in the **BDS**. However, subcontracting of any portion shall not relieve the Bidder from any liability or obligation that may arise from the contract for this Project.

8.2. Subcontractors must submit the documentary requirements under **ITB** Clause 12 and comply with the eligibility criteria specified in the **BDS.** In the event that any subcontractor is found by the Procuring Entity to be ineligible, the subcontracting of such portion of the Goods shall be disallowed.

8.3. The Bidder may identify the subcontractor to whom a portion of the Goods will be subcontracted at any stage of the bidding process or during contract implementation. If the Bidder opts to disclose the name of the subcontractor during bid submission, the Bidder shall include the required documents as part of the technical component of its bid.

B. Contents of Bidding Documents

9. Pre-Bid Conference

9.1. (a) If so specified in the **BDS**, a pre-bid conference shall be held at the venue and on the date indicated therein, to clarify and address the Bidders' questions on the technical and financial components of this Project.

(b) The pre-bid conference shall be held at least twelve (12) calendar days before the deadline for the submission and receipt of bids, but not earlier than seven (7) calendar days from the posting of the invitation to bid/bidding documents in the PhilGEPS website. If the Procuring Entity determines that, by reason of the method, nature, or complexity of the contract to be bid, or when international participation will be more advantageous to the GOP, a longer period for the preparation of bids is necessary, the pre-bid conference shall be held at least thirty (30) calendar days before the deadline for the submission and receipt of bids, as specified in the **BDS**.

9.2. Bidders are encouraged to attend the pre-bid conference to ensure that they fully understand the Procuring Entity's requirements. Non-attendance of the Bidder will in no way prejudice its bid; however, the Bidder is expected to know the changes and/or amendments to the Bidding Documents as recorded in the minutes of the pre-bid conference and the Supplemental/Bid Bulletin. The minutes of the pre-bid conference shall be recorded and prepared not later than five (5) calendar days after the pre-bid conference. The minutes shall be made available to prospective bidders not later than five (5) days upon written request.

9.3 Decisions of the BAC amending any provision of the bidding documents shall be issued in writing through a Supplemental/Bid Bulletin at least seven (7) calendar days before the deadline for the submission and receipt of bids.

10. Clarification and Amendment of Bidding Documents

10.1. Prospective bidders may request for clarification on and/or interpretation of any part of the Bidding Documents. Such request must be in writing and submitted to the Procuring Entity at the address indicated in the **BDS** at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

10.2. The BAC shall respond to the said request by issuing a Supplemental/Bid Bulletin, to be made available to all those who have properly secured the Bidding Documents, at least seven (7) calendar days before the deadline for the submission and receipt of Bids.

10.3. Supplemental/Bid Bulletins may also be issued upon the Procuring Entity's initiative for purposes of clarifying or modifying any provision of the Bidding Documents not later than seven (7) calendar days before the deadline for the submission and receipt of Bids. Any modification to the Bidding Documents shall be identified as an amendment.

10.4. Any Supplemental/Bid Bulletin issued by the BAC shall also be posted in the PhilGEPS and the website of the Procuring Entity concerned, if available, and at any conspicuous place in the premises of the Procuring Entity concerned. It shall be the responsibility of all Bidders who have properly secured the Bidding Documents to inquire and secure Supplemental/Bid Bulletins that may be issued by the BAC. However, Bidders who have submitted bids before the issuance of the Supplemental/Bid Bulletin must be informed and allowed to modify or withdraw their bids in accordance with **ITB** Clause 23.

C. Preparation of Bids

11. Language of Bids

The eligibility requirements or statements, the bids, and all other documents to be submitted to the BAC must be in English. If the eligibility requirements or statements, the bids, and all other documents submitted to the BAC are in foreign language other than English, it must be accompanied by a translation of the documents in English. The documents shall be translated by the relevant foreign government agency, the foreign government agency authorized to translate documents, or a registered translator in the foreign bidder's country; and shall be authenticated by the appropriate Philippine foreign service establishment/post or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. The English translation shall govern, for purposes of interpretation of the bid.

12. Documents Comprising the Bid: Eligibility and Technical Components

1.1. Unless otherwise indicated in the **BDS**, the first envelope shall contain the following eligibility and technical documents:

(a) Eligibility Documents –

Class "A" Documents:

(i) PhilGEPS Certificate of Registration and Membership in accordance with Section 8.5.2 of the IRR, except for foreign bidders participating in the procurement by a Philippine Foreign Service Office or Post, which shall submit their eligibility documents under Section 23.1 of the IRR, provided, that the winning bidder shall register with the PhilGEPS in accordance with section 37.1.4 of the IRR.

(ii) Statement of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid; and

Statement of the Bidder's SLCC similar to the contract to be bid, in accordance with ITB Clause 5.4, within the relevant period as provided in the **BDS.**

The two statements required shall indicate for each contract the following:

(ii.1) name of the contract;

(ii.2) date of the contract;

(ii.3) contract duration;

(ii.4) owner's name and address;

(ii.5) kinds of Goods;

(ii.6) For Statement of Ongoing Contracts - amount of contract and value of outstanding contracts;

(ii.7) For Statement of SLCC - amount of completed contracts, adjusted by the Bidder to current prices using PSA's consumer price index, if necessary for the purpose of meeting the SLCC requirement;

(ii.8) date of delivery; and

(ii.9) end user's acceptance or official receipt(s) or sales invoice issued for the contract, if completed, which shall be attached to the statements.

(iii) NFCC computation in accordance with ITB Clause 5.5 or a committed Line of Credit from a universal or commercial bank.

Class "B" Document:

(iv) If applicable, the Joint Venture Agreement (JVA) in case the joint venture is already in existence, or duly notarized statements from all the potential joint venture partners in accordance with Section 23.1(b) of the IRR.

(b) Technical Documents –

(i) Bid security in accordance with **ITB** Clause 18. If the Bidder opts to submit the bid security in the form of:

(i.1) a bank draft/guarantee or an irrevocable letter of credit issued by a foreign bank, it shall be accompanied by a confirmation from a Universal or Commercial Bank; or

(i.2) a surety bond, it shall be accompanied by a certification by the Insurance Commission that the surety or insurance company is authorized to issue such instruments;

(ii) Conformity with technical specifications, as enumerated and specified in Sections VI and VII of the Bidding Documents; and

(iii) Sworn statement in accordance with Section 25.3 of the IRR of RA 9184 and using the form prescribed in Section VIII. Bidding Forms..

(iv) For foreign bidders claiming eligibility by reason of their country's extension of reciprocal rights to Filipinos, a certification from the relevant government office of their country stating that Filipinos are allowed to participate in their government procurement activities for the same item or product.

2. Documents Comprising the Bid: Financial Component

2.1. Unless otherwise stated in the **BDS**, the financial component of the bid shall contain the following:

(a) Financial Bid Form, which includes bid prices and the applicable Price Schedules, in accordance with **ITB** Clauses 15.1 and 15.4;

(b) If the Bidder claims preference as a Domestic Bidder, a certification from the DTI issued in accordance with **ITB** Clause 27, unless otherwise provided in the **BDS**; and

(c) Any other document related to the financial component of the bid as stated in the **BDS**.

2.2. (a) Unless otherwise stated in the **BDS,** all bids that exceed the ABC shall not be accepted.

(b) Unless otherwise indicated in the **BDS**, for foreign-funded procurement, a ceiling may be applied to bid prices provided the following conditions are met:

(i) Bidding Documents are obtainable free of charge on a freely accessible website. If payment of Bidding Documents is required by the procuring entity, payment could be made upon the submission of bids.

(ii) The procuring entity has procedures in place to ensure that the ABC is based on recent estimates made by the responsible unit of the procuring entity and that the estimates reflect the quality, supervision and risk and inflationary factors, as well as prevailing market prices, associated with the types of works or goods to be procured.

(iii) The procuring entity has trained cost estimators on estimating prices and analyzing bid variances.

(iv) The procuring entity has established a system to monitor and report bid prices relative to ABC and engineer's/procuring entity's estimate.

(v) The procuring entity has established a monitoring and evaluation system for contract implementation to provide a feedback on actual total costs of goods and works.

3. Alternative Bids

14.1 Alternative Bids shall be rejected. For this purpose, alternative bid is an offer made by a Bidder in addition or as a substitute to its original bid which may be included as part of its original bid or submitted separately therewith for purposes of bidding. A bid with options is considered an alternative bid regardless of whether said bid proposal is contained in a single envelope or submitted in two (2) or more separate bid envelopes.

14.2 Each Bidder shall submit only one Bid, either individually or as a partner in a JV. A Bidder who submits or participates in more than one bid (other than as a subcontractor if a subcontractor is permitted to participate in more than one bid) will cause all the proposals with the Bidder's participation to be disqualified. This shall be without prejudice to any applicable criminal, civil and administrative penalties that may be imposed upon the persons and entities concerned.

4. Bid Prices

4.1. The Bidder shall complete the appropriate Schedule of Prices included herein, stating the unit prices, total price per item, the total amount and the expected countries of origin of the Goods to be supplied under this Project.

4.2. The Bidder shall fill in rates and prices for all items of the Goods described in the Schedule of Prices. Bids not addressing or providing all of the required items in the Bidding Documents including, where applicable, Schedule of Prices, shall be considered non-responsive and, thus, automatically disqualified. In this regard, where a required item is provided, but no price is indicated, the same shall be considered as non-responsive, but specifying a zero (0) or a dash (-) for the said item would mean that it is being offered for free to the Government, except those required by law or regulations to be accomplished.

4.3. The terms Ex Works (EXW), Cost, Insurance and Freight (CIF), Cost and Insurance Paid to (CIP), Delivered Duty Paid (DDP), and other trade terms used to describe the obligations of the parties, shall be governed by the rules prescribed in the current edition of the International Commercial Terms (INCOTERMS) published by the International Chamber of Commerce, Paris.

4.4. Prices indicated on the Price Schedule shall be entered separately in the following manner:

(a) For Goods offered from within the Procuring Entity's country:

(i) The price of the Goods quoted EXW (ex works, ex factory, ex warehouse, ex showroom, or off-the-shelf, as applicable);

(ii) The cost of all customs duties and sales and other taxes already paid or payable;

(iii) The cost of transportation, insurance, and other costs incidental to delivery of the Goods to their final destination; and

(iv) The price of other (incidental) services, if any, listed in the **BDS**.

(b) For Goods offered from abroad:

(i) Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted DDP with the place of destination in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.

(ii) The price of other (incidental) services, if any, listed in the **BDS**.

(c) For Services, based on the form which may be prescribed by the Procuring Entity, in accordance with existing laws, rules and regulations

4.5. Prices quoted by the Bidder shall be fixed during the Bidder's performance of the contract and not subject to variation or price escalation on any account. A bid submitted with an adjustable price quotation shall be treated as non-responsive and shall be rejected, pursuant to **ITB** Clause 24.

All bid prices for the given scope of work in the contract as awarded shall be considered as fixed prices, and therefore not subject to price escalation during contract implementation, except under extraordinary circumstances. Upon the recommendation of the Procuring Entity, price escalation may be allowed in extraordinary circumstances as may be determined by the National Economic and Development Authority in accordance with the Civil Code of the Philippines, and upon approval by the GPPB. Nevertheless, in cases where the cost of the awarded contract is affected by any applicable new laws, ordinances, regulations, or other acts of the GOP, promulgated after the date of bid opening, a contract price adjustment shall be made or appropriate relief shall be applied on a no loss-no gain basis.

5. Bid Currencies

5.1. Prices shall be quoted in the following currencies:

(a) For Goods that the Bidder will supply from within the Philippines, the prices shall be quoted in Philippine Pesos.

(b) For Goods that the Bidder will supply from outside the Philippines, the prices may be quoted in the currency(ies) stated in the **BDS**. However, for purposes of bid evaluation, bids denominated in foreign currencies shall be converted to Philippine currency based on the exchange rate as published in the *Bangko Sentral ng Pilipinas* (BSP) reference rate bulletin on the day of the bid opening.

5.2. If so allowed in accordance with **ITB** Clause 16.1, the Procuring Entity for purposes of bid evaluation and comparing the bid prices will convert the amounts in various currencies in which the bid price is expressed to Philippine Pesos at the foregoing exchange rates.

5.3. Unless otherwise specified in the **BDS**, payment of the contract price shall be made in Philippine Pesos.

6. Bid Validity

6.1. Bids shall remain valid for the period specified in the **BDS** which shall not exceed one hundred twenty (120) calendar days from the date of the opening of bids.

6.2. In exceptional circumstances, prior to the expiration of the bid validity period, the Procuring Entity may request Bidders to extend the period of validity of their bids. The request and the responses shall be made in writing. The bid security described in **ITB** Clause 18 should also be extended corresponding to the extension of the bid validity period at the least. A Bidder may refuse the request without forfeiting its bid security, but his bid shall no longer be considered for further evaluation and award. A Bidder granting the request shall not be required or permitted to modify its bid.

7. Bid Security

7.1. The Bidder shall submit a Bid Securing Declaration or any form of Bid Security in the amount stated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the following schedule:

Form of Bid Security	Amount of Bid Security (Not Less than the Percentage of the ABC)
(a) Cash or cashier's/manager's check issued by a Universal or Commercial Bank. *For biddings conducted by LGUs, the Cashier's/Manager's Check may be issued by other banks certified by the BSP as authorized to issue such financial instrument.*	Two percent (2%)
(b) Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank. *For biddings conducted by LGUs, Bank Draft/Guarantee, or Irrevocable Letter of Credit may be issued by other banks certified by the BSP as authorized to issue such financial instrument.*	
(c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	Five percent (5%)

The Bid Securing Declaration mentioned above is an undertaking which states, among others, that the Bidder shall enter into contract with the procuring entity and furnish the performance security required under ITB Clause 33.2, within ten (10) calendar days from receipt of the Notice of Award, and commits to pay the corresponding amount as fine, and be suspended for a period of time from being qualified to participate in any government procurement activity in the event it violates any of the conditions stated therein as provided in the guidelines issued by the GPPB.

7.2. The bid security should be valid for the period specified in the **BDS**. Any bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

7.3. No bid securities shall be returned to Bidders after the opening of bids and before contract signing, except to those that failed or declared as post-disqualified, upon submission of a written waiver of their right to file a request for reconsideration and/or protest, or upon the lapse of the reglementary period to file a request for reconsideration or protest. Without prejudice on its forfeiture, bid securities shall be returned only after the Bidder with the Lowest Calculated Responsive Bid (LCRB) has signed the contract and furnished the performance security, but in no case later than the expiration of the bid security validity period indicated in **ITB** Clause 18.2.

7.4. Upon signing and execution of the contract pursuant to **ITB** Clause 32, and the posting of the performance security pursuant to **ITB** Clause 33, the successful Bidder's bid security will be discharged, but in no case later than the bid security validity period as indicated in the **ITB** Clause 18.2.

7.5. The bid security may be forfeited:

(a) if a Bidder:

(i) withdraws its bid during the period of bid validity specified in **ITB** Clause 17;

(ii) does not accept the correction of errors pursuant to **ITB** Clause 28.3(b);

(iii) has a finding against the veracity of any of the documents submitted as stated in **ITB** Clause 29.2;

(iv) submission of eligibility requirements containing false information or falsified documents;

(v) submission of bids that contain false information or falsified documents, or the concealment of such information in the bids in order to influence the outcome of eligibility screening or any other stage of the public bidding;

(vi) allowing the use of one's name, or using the name of another for purposes of public bidding;

(vii) withdrawal of a bid, or refusal to accept an award, or enter into contract with the Government without justifiable cause, after the Bidder had been adjudged as having submitted the LCRB;

(viii) refusal or failure to post the required performance security within the prescribed time;

(ix) refusal to clarify or validate in writing its bid during post-qualification within a period of seven (7) calendar days from receipt of the request for clarification;

(x) any documented attempt by a Bidder to unduly influence the outcome of the bidding in his favor;

(xi) failure of the potential joint venture partners to enter into the joint venture after the bid is declared successful; or

(xii) all other acts that tend to defeat the purpose of the competitive bidding, such as habitually withdrawing from bidding, submitting late Bids or patently insufficient bid, for at least three (3) times within a year, except for valid reasons.

(b) if the successful Bidder:

(i) fails to sign the contract in accordance with **ITB** Clause 32; or

(ii) fails to furnish performance security in accordance with **ITB** Clause 33.

8. Format and Signing of Bids

8.1. Bidders shall submit their bids through their duly authorized representative using the appropriate forms provided in Section VIII. Bidding Forms on or before the deadline specified in the **ITB** Clauses 21 in two (2) separate sealed bid envelopes, and which shall be submitted simultaneously. The first shall contain the technical component of the bid, including the eligibility requirements under **ITB** Clause 12.1, and the second shall contain the financial component of the bid. This shall also be observed for each lot in the case of lot procurement.

8.2. Forms as mentioned in **ITB** Clause 19.1 must be completed without any alterations to their format, and no substitute form shall be accepted. All blank spaces shall be filled in with the information requested.

8.3. The Bidder shall prepare and submit an original of the first and second envelopes as described in **ITB** Clauses 12 and 13. In addition, the Bidder shall submit copies of the first and second envelopes. In the event of any discrepancy between the original and the copies, the original shall prevail.

8.4. Each and every page of the Bid Form, including the Schedule of Prices, under Section VIII hereof, shall be signed by the duly authorized representative/s of the Bidder. Failure to do so shall be a ground for the rejection of the bid.

8.5. Any interlineations, erasures, or overwriting shall be valid only if they are signed or initialed by the duly authorized representative/s of the Bidder.

9. Sealing and Marking of Bids

9.1. Bidders shall enclose their original eligibility and technical documents described in **ITB** Clause 12 in one sealed envelope marked "ORIGINAL - TECHNICAL COMPONENT", and the original of their financial component in another sealed envelope marked "ORIGINAL - FINANCIAL COMPONENT", sealing them all in an outer envelope marked "ORIGINAL BID".

9.2. Each copy of the first and second envelopes shall be similarly sealed duly marking the inner envelopes as "COPY NO. ___ - TECHNICAL COMPONENT" and "COPY NO. ___ – FINANCIAL COMPONENT" and the outer envelope as "COPY NO. ___", respectively. These envelopes containing the original and the copies shall then be enclosed in one single envelope.

9.3. The original and the number of copies of the Bid as indicated in the **<u>BDS</u>** shall be typed or written in ink and shall be signed by the Bidder or its duly authorized representative/s.

9.4. All envelopes shall:

(a) contain the name of the contract to be bid in capital letters;

(b) bear the name and address of the Bidder in capital letters;

(c) be addressed to the Procuring Entity's BAC in accordance with **ITB** Clause 1.1;

(d) bear the specific identification of this bidding process indicated in the **ITB** Clause 1.2; and

(e) bear a warning "DO NOT OPEN BEFORE…" the date and time for the opening of bids, in accordance with **ITB** Clause 21.

9.5. Bid envelopes that are not properly sealed and marked, as required in the bidding documents, shall not be rejected, but the Bidder or its duly authorized representative shall acknowledge such condition of the bid as submitted. The BAC or the Procuring Entity shall assume no responsibility for the misplacement of the contents of the improperly sealed or marked bid, or for its premature opening.

D. Submission and Opening of Bids

10. Deadline for Submission of Bids

Bids must be received by the Procuring Entity's BAC at the address and on or before the date and time indicated in the **<u>BDS</u>**.

11. Late Bids

Any bid submitted after the deadline for submission and receipt of bids prescribed by the Procuring Entity, pursuant to **ITB** Clause 21, shall be declared "Late" and shall not be accepted by the Procuring Entity. The BAC shall record in the minutes of bid submission and opening, the Bidder's name, its representative and the time the late bid was submitted.

12. Modification and Withdrawal of Bids

12.1. The Bidder may modify its bid after it has been submitted; provided that the modification is received by the Procuring Entity prior to the deadline prescribed for submission and receipt of bids. The Bidder shall not be allowed to retrieve its original bid, but shall be allowed to submit another bid equally sealed and properly identified in accordance with ITB Clause 20, linked to its original bid marked as "TECHNICAL MODIFICATION" or "FINANCIAL MODIFICATION" and stamped "received" by the BAC. Bid modifications received after the applicable deadline shall not be considered and shall be returned to the Bidder unopened.

23.2 A Bidder may, through a Letter of Withdrawal, withdraw its bid after it has been submitted, for valid and justifiable reason; provided that the Letter of Withdrawal is received by the Procuring Entity prior to the deadline prescribed for submission and receipt of bids. The Letter of Withdrawal must be executed by the duly authorized representative of the Bidder identified in the Omnibus Sworn Statement, a copy of which should be attached to the letter.

12.2.

12.3. Bids requested to be withdrawn in accordance with **ITB** Clause 23.1 shall be returned unopened to the Bidders. A Bidder, who has acquired the bidding documents, may also express its intention not to participate in the bidding through a letter which should reach and be stamped by the BAC before the deadline for submission and receipt of bids. A Bidder that withdraws its bid shall not be permitted to submit another bid, directly or indirectly, for the same contract.

12.4. No bid may be modified after the deadline for submission of bids. No bid may be withdrawn in the interval between the deadline for submission of bids and the expiration of the period of bid validity specified by the Bidder on the Financial Bid Form. Withdrawal of a bid during this interval shall result in the forfeiture of the Bidder's bid security, pursuant to **ITB** Clause 18.5, and the imposition of administrative, civil and criminal sanctions as prescribed by RA 9184 and its IRR.

13. Opening and Preliminary Examination of Bids

13.1. The BAC shall open the bids in public, immediately after the deadline for the submission and receipt of bids, as specified in the **BDS**. In case the Bids cannot be opened as scheduled due to justifiable reasons, the BAC shall take custody of the Bids submitted and reschedule the opening of Bids on the next working day or at the soonest possible time through the issuance of a Notice of Postponement to be posted in the PhilGEPS website and the website of the Procuring Entity concerned.

13.2. Unless otherwise specified in the **BDS**, the BAC shall open the first bid envelopes and determine each Bidder's compliance with the documents prescribed in **ITB** Clause 12, using a non-discretionary "pass/fail" criterion. If a Bidder submits the required document, it shall be rated "passed" for that particular requirement. In this regard, bids that fail to include any requirement or are incomplete or patently insufficient shall be considered as "failed". Otherwise, the BAC shall rate the said first bid envelope as "passed".

13.3. Unless otherwise specified in the **BDS**, immediately after determining compliance with the requirements in the first envelope, the BAC shall forthwith open the second bid envelope of each remaining eligible bidder whose first bid envelope was rated "passed". The second envelope of each complying bidder shall be opened within the same day. In case one or more of the requirements in the second envelope of a particular bid is missing, incomplete or patently insufficient, and/or if the submitted total bid price exceeds the ABC unless otherwise provided in **ITB** Clause 13.2, the BAC shall rate the bid concerned as "failed". Only bids that are determined to contain all the bid requirements for both components shall be rated "passed" and shall immediately be considered for evaluation and comparison.

13.4. Letters of Withdrawal shall be read out and recorded during bid opening, and the envelope containing the corresponding withdrawn bid shall be returned to the Bidder unopened.

13.5. All members of the BAC who are present during bid opening shall initial every page of the original copies of all bids received and opened.

13.6. In the case of an eligible foreign bidder as described in **ITB** Clause 5, the following Class "A" Documents may be substituted with the appropriate equivalent documents, if any, issued by the country of the foreign Bidder concerned, which shall likewise be uploaded and maintained in the PhilGEPS in accordance with Section 8.5.2 of the IRR:

(a) Registration certificate from the Securities and Exchange Commission (SEC), Department of Trade and Industry (DTI) for sole proprietorship, or CDA for cooperatives;

(b) Mayor's/Business permit issued by the local government where the priCMSPal place of business of the bidder is located; and

(c) Audited Financial Statements showing, among others, the prospective bidder's total and current assets and liabilities stamped "received" by the Bureau of Internal Revenue or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two years from the date of bid submission.

13.7. Each partner of a joint venture agreement shall likewise submit the requirements in **ITB** Clause 12.1(a)(i). Submission of documents required under **ITB** Clauses 12.1(a)(ii) to 12.1(a)(iii) by any of the joint venture partners constitutes compliance.

13.8. The Procuring Entity shall prepare the minutes of the proceedings of the bid opening that shall include, as a minimum: (a) names of Bidders, their bid price (per lot, if applicable, and/or including discount, if any), bid security, findings of preliminary examination, and whether there is a withdrawal or modification; and (b) attendance sheet. The BAC members shall sign the abstract of bids as read.

24.8 The bidders or their duly authorized representatives may attend the opening of bids. The BAC shall ensure the integrity, security, and confidentiality of all submitted bids. The Abstract of Bids as read and the minutes of the bid opening shall be made available to the public upon written request and payment of a specified fee to recover cost of materials.

24.9 To ensure transparency and accurate representation of the bid submission, the BAC Secretariat shall notify in writing all bidders whose bids it has received through its PhilGEPS-registered physical address or official e-mail address. The notice shall be issued within seven (7) calendar days from the date of the bid opening.

E. Evaluation and Comparison of Bids

14. Process to be Confidential

14.1. Members of the BAC, including its staff and personnel, as well as its Secretariat and TWG, are prohibited from making or accepting any kind of communication with any bidder regarding the evaluation of their bids until the issuance of the Notice of Award, unless otherwise allowed in the case of **ITB** Clause 26.

14.2. Any effort by a bidder to influence the Procuring Entity in the Procuring Entity's decision in respect of bid evaluation, bid comparison or contract award will result in the rejection of the Bidder's bid.

15. Clarification of Bids

To assist in the evaluation, comparison, and post-qualification of the bids, the Procuring Entity may ask in writing any Bidder for a clarification of its bid. All responses to requests for clarification shall be in writing. Any clarification submitted by a Bidder in respect to its bid and that is not in response to a request by the Procuring Entity shall not be considered.

16. Domestic Preference

16.1. Unless otherwise stated in the **BDS**, the Procuring Entity will grant a margin of preference for the purpose of comparison of bids in accordance with the following:

(a) The preference shall be applied when the lowest Foreign Bid is lower than the lowest bid offered by a Domestic Bidder.

(b) For evaluation purposes, the lowest Foreign Bid shall be increased by fifteen percent (15%).

(c) In the event that the lowest bid offered by a Domestic Bidder does not exceed the lowest Foreign Bid as increased, then the Procuring Entity shall award the contract to the Domestic Bidder at the amount of the lowest Foreign Bid.

(d) If the Domestic Bidder refuses to accept the award of contract at the amount of the Foreign Bid within two (2) calendar days from receipt of written advice from the BAC, the Procuring Entity shall award to the bidder offering the Foreign Bid, subject to post-qualification and submission of all the documentary requirements under these Bidding Documents.

16.2. A Bidder may be granted preference as a Domestic Bidder subject to the certification from the DTI that the Bidder is offering unmanufactured articles, materials or supplies of the growth or production of the Philippines, or manufactured articles, materials, or supplies manufactured or to be manufactured in the Philippines substantially from articles, materials, or supplies of the growth, production, or manufacture, as the case may be, of the Philippines.

17. Detailed Evaluation and Comparison of Bids

17.1. The Procuring Entity will undertake the detailed evaluation and comparison of bids which have passed the opening and preliminary examination of bids, pursuant to **ITB** Clause 24, in order to determine the Lowest Calculated Bid.

17.2. The Lowest Calculated Bid shall be determined in two steps:

(a) The detailed evaluation of the financial component of the bids, to establish the correct calculated prices of the bids; and

(b) The ranking of the total bid prices as so calculated from the lowest to the highest. The bid with the lowest price shall be identified as the Lowest Calculated Bid.

17.3. The Procuring Entity's BAC shall immediately conduct a detailed evaluation of all bids rated "passed," using non-discretionary pass/fail criteria. The BAC shall consider the following in the evaluation of bids:

(a) Completeness of the bid. Unless the **BDS** allows partial bids, bids not addressing or providing all of the required items in the Schedule of Requirements including, where applicable, Schedule of Prices, shall be considered non-responsive and, thus, automatically disqualified. In this regard, where a required item is provided, but no price is indicated, the same shall be considered as non-responsive, but specifying a zero (0) or a dash (-) for the said item would mean that it is being offered for free to the Procuring Entity, except those required by law or regulations to be provided for; and

(b) Arithmetical corrections. Consider computational errors and omissions to enable proper comparison of all eligible bids. It may also consider bid modifications. Any adjustment shall be calculated in monetary terms to determine the calculated prices.

17.4. Based on the detailed evaluation of bids, those that comply with the above-mentioned requirements shall be ranked in the ascending order of their total calculated bid prices, as evaluated and corrected for computational errors, discounts and other modifications, to identify the Lowest Calculated Bid. Total calculated bid prices, as evaluated and corrected for computational errors, discounts and other modifications, which exceed the ABC shall not be considered, unless otherwise indicated in the **BDS**.

17.5. The Procuring Entity's evaluation of bids shall be based on the bid price quoted in the Bid Form, which includes the Schedule of Prices.

17.6. Bids shall be evaluated on an equal footing to ensure fair competition. For this purpose, all bidders shall be required to include in their bids the cost of all taxes, such as, but not limited to, value added tax (VAT), income tax, local taxes, and other fiscal levies and duties which shall be itemized in the bid form and reflected in the detailed estimates. Such bids, including said taxes, shall be the basis for bid evaluation and comparison.

17.7. If so indicated pursuant to **ITB** Clause 1.2, Bids are being invited for individual lots or for any combination thereof, provided that all Bids and combinations of Bids shall be received by the same deadline and opened and evaluated simultaneously so as to determine the Bid or combination of Bids offering the lowest calculated cost to the Procuring Entity. Bid prices quoted shall correspond to all items specified for each lot and to all quantities specified for each item of a lot. Bid Security as required by **ITB** Clause 18 shall be submitted for each contract (lot) separately. The basis for evaluation of lots is specified in BDS Clause 28.3.

18. Post-Qualification

18.1. The BAC shall determine to its satisfaction whether the Bidder that is evaluated as having submitted the Lowest Calculated Bid complies with and is responsive to all the requirements and conditions specified in **ITB** Clauses 5, 12, and 13.

18.2. Within a non-extendible period of five (5) calendar days from receipt by the bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

Failure to submit any of the post-qualification requirements on time, or a finding against the veracity thereof, shall disqualify the bidder for award. Provided in the event that a finding against the veracity of any of the documents submitted is made, it shall cause the forfeiture of the bid security in accordance with Section 69 of the IRR of RA 9184.

18.3. The determination shall be based upon an examination of the documentary evidence of the Bidder's qualifications submitted pursuant to **ITB** Clauses 12 and 13, as well as other information as the Procuring Entity deems necessary and appropriate, using a non-discretionary "pass/fail" criterion, which shall be completed within a period of twelve (12) calendar days.

18.4. If the BAC determines that the Bidder with the Lowest Calculated Bid passes all the criteria for post-qualification, it shall declare the said bid as the LCRB, and recommend to the HoPE the award of contract to the said Bidder at its submitted price or its calculated bid price, whichever is lower.

18.5. A negative determination shall result in rejection of the Bidder's Bid, in which event the Procuring Entity shall proceed to the next Lowest Calculated Bid with a fresh period to make a similar determination of that Bidder's capabilities to perform satisfactorily. If the second Bidder, however, fails the post qualification, the procedure for post qualification shall be repeated for the Bidder with the next Lowest Calculated Bid, and so on until the LCRB is determined for recommendation for contract award.

18.6. Within a period not exceeding fifteen (15) calendar days from the determination by the BAC of the LCRB and the recommendation to award the contract, the HoPE or his duly authorized representative shall approve or disapprove the said recommendation.

18.7. In the event of disapproval, which shall be based on valid, reasonable, and justifiable grounds as provided for under Section 41 of the IRR of RA 9184, the HoPE shall notify the BAC and the Bidder in writing of such decision and the grounds for it. When applicable, the BAC shall conduct a post-qualification of the Bidder with the next Lowest Calculated Bid. A request for reconsideration may be filed by the bidder with the HoPE in accordance with Section 37.1.3 of the IRR of RA 9184.

19. Reservation Clause

19.1. Notwithstanding the eligibility or post-qualification of a Bidder, the Procuring Entity concerned reserves the right to review its qualifications at any stage of the procurement process if it has reasonable grounds to believe that a misrepresentation has been made by the said Bidder, or that there has been a change in the Bidder's capability to undertake the project from the time it submitted its eligibility requirements. Should such review uncover any misrepresentation made in the eligibility and bidding requirements, statements or documents, or any changes in the situation of the Bidder which will affect its capability to undertake the project so that it fails the preset eligibility or bid evaluation criteria, the Procuring Entity shall consider the said Bidder as ineligible and shall disqualify it from submitting a bid or from obtaining an award or contract.

19.2. Based on the following grounds, the Procuring Entity reserves the right to reject any and all bids, declare a Failure of Bidding at any time prior to the contract award, or not to award the contract, without thereby incurring any liability, and make no assurance that a contract shall be entered into as a result of the bidding:

(a) If there is *prima facie* evidence of collusion between appropriate public officers or employees of the Procuring Entity, or between the BAC and any of the Bidders, or if the collusion is between or among the bidders themselves, or between a Bidder and a third party, including any act which restricts, suppresses or nullifies or tends to restrict, suppress or nullify competition;

(b) If the Procuring Entity's BAC is found to have failed in following the prescribed bidding procedures; or

(c) For any justifiable and reasonable ground where the award of the contract will not redound to the benefit of the GOP as follows:

(i) If the physical and economic conditions have significantly changed so as to render the project no longer economically, financially or technically feasible as determined by the HoPE;

(ii) If the project is no longer necessary as determined by the HoPE; and

(iii) If the source of funds for the project has been withheld or reduced through no fault of the Procuring Entity.

19.3. In addition, the Procuring Entity may likewise declare a failure of bidding when:

(a) No bids are received;

(b) All prospective Bidders are declared ineligible;

(c) All bids fail to comply with all the bid requirements or fail post-qualification; or

(d) The bidder with the LCRB refuses, without justifiable cause to accept the award of contract, and no award is made in accordance with Section 40 of the IRR of RA 9184.

F. Award of Contract

20. Contract Award

20.1. Subject to **ITB** Clause 29, the HoPE or its duly authorized representative shall award the contract to the Bidder whose bid has been determined to be the LCRB.

20.2. Prior to the expiration of the period of bid validity, the Procuring Entity shall notify the successful Bidder in writing that its bid has been accepted, through a Notice of Award duly received by the Bidder or its representative personally or sent by registered mail or electronically, receipt of which must be confirmed in writing within two (2) days by the Bidder with the LCRB and submitted personally or sent by registered mail or electronically to the Procuring Entity.

20.3. Notwithstanding the issuance of the Notice of Award, award of contract shall be subject to the following conditions:

(a) Submission of the following documents within ten (10) calendar days from receipt of the Notice of Award:

(i) Valid JVA, if applicable; or

(ii) In the case of procurement by a Philippine Foreign Service Office or Post, the PhilGEPS Registration Number of the winning foreign Bidder;

(b) Posting of the performance security in accordance with **ITB** Clause 33;

(c) Signing of the contract as provided in **ITB** Clause 32; and

(d) Approval by higher authority, if required, as provided in Section 37.3 of the IRR of RA 9184.

20.4. At the time of contract award, the Procuring Entity shall not increase or decrease the quantity of goods originally specified in Section VI. Schedule of Requirements.

21. Signing of the Contract

21.1. At the same time as the Procuring Entity notifies the successful Bidder that its bid has been accepted, the Procuring Entity shall send the Contract Form to the Bidder, which contract has been provided in the Bidding Documents, incorporating therein all agreements between the parties.

21.2. Within ten (10) calendar days from receipt of the Notice of Award, the successful Bidder shall post the required performance security, sign and date the contract and return it to the Procuring Entity.

21.3. The Procuring Entity shall enter into contract with the successful Bidder within the same ten (10) calendar day period provided that all the documentary requirements are complied with.

21.4. The following documents shall form part of the contract:

(a) Contract Agreement;

(b) Bidding Documents;

(c) Winning bidder's bid, including the Technical and Financial Proposals, and all other documents/statements submitted (*e.g.,* bidder's response to request for clarifications on the bid), including corrections to the bid, if any, resulting from the Procuring Entity's bid evaluation;

(d) Performance Security;

(e) Notice of Award of Contract; and

(f) Other contract documents that may be required by existing laws and/or specified in the **BDS**.

22. Performance Security

22.1. To guarantee the faithful performance by the winning Bidder of its obligations under the contract, it shall post a performance security within a maximum period of ten (10) calendar days from the receipt of the Notice of Award from the Procuring Entity and in no case later than the signing of the contract.

22.2. The Performance Security shall be denominated in Philippine Pesos and posted in favor of the Procuring Entity in an amount not less than the percentage of the total contract price in accordance with the following schedule:

Form of Performance Security	Amount of Performance Security (Not less than the Percentage of the Total Contract Price)
(a) Cash or cashier's/manager's check issued by a Universal or Commercial Bank. *For biddings conducted by the LGUs, the Cashier's/Manager's Check may be issued by other banks certified by the BSP as authorized to issue such financial instrument.*	Five percent (5%)

(b)	Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank. *For biddings conducted by the LGUs, the Bank Draft/ Guarantee or Irrevocable Letter of Credit may be issued by other banks certified by the BSP as authorized to issue such financial instrument.*	
(c)	Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	Thirty percent (30%)

22.3. Failure of the successful Bidder to comply with the above-mentioned requirement shall constitute sufficient ground for the annulment of the award and forfeiture of the bid security, in which event the Procuring Entity shall have a fresh period to initiate and complete the post qualification of the second Lowest Calculated Bid. The procedure shall be repeated until the LCRB is identified and selected for recommendation of contract award. However if no Bidder passed post-qualification, the BAC shall declare the bidding a failure and conduct a re-bidding with re-advertisement, if necessary.

23. Notice to Proceed

Within seven (7) calendar days from the date of approval of the contract by the appropriate government approving authority, the Procuring Entity shall issue the Notice to Proceed (NTP) together with a copy or copies of the approved contract to the successful Bidder. All notices called for by the terms of the contract shall be effective only at the time of receipt thereof by the successful Bidder.

24. Protest Mechanism

Decisions of the procuring entity at any stage of the procurement process may be questioned in accordance with Section 55 of the IRR of RA 9184.

Section III.
Bid Data Sheet (BDS)

Bid Data Sheet

ITB Clause	
1.1	The Procuring Entity is the **DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY (DICT)** The name of the Contract is **SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT**
1.2	The lot and reference is: **BAC4G&S-2018-002** **SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT**
2	The Funding Source is: The Government of the Philippines (GOP) through the **2018 GAA** in the amount of **Five Hundred Twelve Million Pesos (PhP512,000,000.00).** The name of the Project is: **SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT**
3.1	No further instructions.
5.1	No further instructions.
5.2	Foreign bidders, except those falling under **ITB** Clause 5.2(b), may not participate in this Project.
5.4	The Bidder must have completed, within the last five (5) years from the date of submission and receipt of at least one (1) single contract of similar nature amounting to at least fifty percent (50%) of the ABC. For this project, "similar in nature" shall mean "Security Operations Center (SOC)".
7	No further instructions.
8.1	Subcontracting is not allowed.
8.2	Not applicable.
9.1	The Procuring Entity will hold a **Pre-Bid Conference** for this Project on **7 June 2018, 1:30PM** at **Executive Lounge, DICT Building, C.P. Garcia Avenue, Diliman, Quezon City.**
10.1	The Procuring Entity's address is: **Department of Information and Communications Technology** DICT Building, C.P. Garcia Avenue, Diliman, Quezon City **Engr. Thelma D. Villamorel** Head, BAC Secretariat

	Department of Information and Communications Technology C.P. Garcia Avenue, Diliman, Quezon City Telephone No.: 920-0101 local 1831 Email Address: bac4g&s@dict.gov.ph Website: **www.dict.gov.ph**
12	**In accordance with Clause 19.4 of the Instructions to Bidders, the bid, except for the unamended printed literature, shall be signed, and each and every page thereof shall be initialed, by the duly authorized representative/s to the Bidder.** (a) **ELIGIBILITY DOCUMENTS –** **Class "A" Documents:** i. Registration Certificate from the Securities and Exchange Commission (SEC) for corporations, Department of Trade and Industry (DTI) for sole proprietorship, or from Cooperative Development Authority CDA) for cooperatives; ii. Valid and Current Business/Mayor's Permit issued by the city or municipality where the principal place of business of the prospective bidder is located OR the equivalent document for Exclusive Economic Zones or Areas; In cases of recently expired Mayor's / Business Permits, said permit shall be submitted together with the official receipt as proof that the bidder has applied for renewal with the period prescribed by the concerned local government units, provided that the renewed permit shall be submitted as a post-qualification requirement. iii. Valid and Current Tax Clearance issued by Philippines' Bureau of Internal Revenue (BIR) Accounts Receivable Monitoring Division per Executive Order 398, Series of 2005; iv. Copy of each of the following Audited Financial Statements for 2017 and 2016 (in comparative format or separate reports): a. Independent Auditor's Report; b. Balance Sheet (Statement of Financial Position); and c. Income Statement (Statement of Comprehensive Income)

OR

Submission of valid and current PHILGEPS Certificate of Registration and Membership (Platinum Registration) together with Annex A in lieu of (Items i., ii., iii., iv.) Eligibility Documents.

Note: Bidder must ensure that all Class "A" Eligibility Documents are valid and current at the time of submission of PHILGEPS Certificate of Registration and Membership (Platinum Registration). In case any of the submitted Eligibility Documents are not valid and current at the time of submission of Platinum Registration, bidders are required to submit the valid and current documents together with the Platinum Registration.

In case the bidder opt to submit their Class "A" Documents, the Certificate of PhilGEPS Registration (Platinum Membership) shall remain as post-qualification requirement to be submitted in accordance with Section 34.2 of the 2016 Revised IRR of RA9184. "GPPB Circular 07-2017 dated 31 July 2017".

v. Statement of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid **(Annex I);**

vi. Statement of Completed Single Largest Contract of Similar Nature within the last five (5) years from the date of submission and receipt of bids equivalent to at least fifty percent (50%) of the ABC **(Annex I-A).**

"Similar" contract shall refer to Security Operations Center (SOC).

Any of the following documents must be submitted corresponding to listed contracts per submitted Annex I-A:

a. Copy of End user's acceptance;
b. Copy of Official receipt/s; or
c. Copy of Sales Invoice

vii. Duly signed Net Financial Contracting Capacity Computation (NFCC)* per **Annex II,** in accordance with ITB Clause 5.5 or a committed Line of Credit equivalent to at least ten percent (10%) of the ABC from a universal or commercial bank.

a. Should the bidder opt to submit NFCC, computation must be equal to the ABC of the project.

*NFCC = [(Current Assets minus Current Liabilities) (15)] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started coinciding with the contract to be bid.

Notes:

A. The values of the bidder's current assets and current liabilities shall be based on the data submitted to BIR through its Electronic Filing and Payment System.
B. Value of all outstanding or uncompleted contracts refers those listed in Annex-I.
C. The detailed computation using the required formula must be shown as provided above.
D. The NFCC computation must at least be equal to the total ABC of the project.

OR

b. Should the bidder opt to submit a Committed Line of Credit, it must be at least equal to ten percent (10%) of the ABC issued by a Local Universal or Local Commercial Bank.

Class "B" Documents: (For Joint Ventures)

viii. For Joint Ventures, Bidders to submit either:

1. Copy of the JOINT VENTURE AGREEMENT (JVA) in case the joint venture is already in existence; or

2. Copy of Protocol / Undertaking of Agreement to Enter into Joint Venture signed by all the potential join venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful. **(Annex III)**

   The JVA or the Protocol/Undertaking of Agreement to Enter into Joint Venture (Annex III) must include/specify the company/partner and the name of the office designated as authorized representative of the Joint Venture.q

For Joint Venture, the following documents must likewise be submitted by each partner:

1. Registration Certificate from the Securities and Exchange Commission (SEC) for corporations or from Department of Trade and Industry (DTI) for sole proprietorship, or from Cooperative Development Authority (CDA) for cooperatives;

2. Valid and Current Business/Mayor's Permit issued by the city or municipality where the principal place of business of the prospective bidder is located OR the equivalent document for Exclusive Economic Zones or Areas;

   In cases of recently expired Mayor's / Business Permits, said permit shall be submitted together with the official receipt as proof that the bidder has applied for renewal with the period prescribed by the concerned local government units, provided that the renewed permit shall be submitted as a post-qualification requirement;

3. Valid and current Tax Clearance issued by Philippines' Bureau of Internal Revenue (BIR) Accounts Receivable Monitoring Division per Executive Order 398, Series of 2005;

4. Copy of each of the following Audited Financial Statements for 2016 and 2015 (in comparative form or separate reports):

   a. Independent Auditor's Report;

   b. Balance Sheet (Statement of Financial Position); and

   c. Income Statement (Statement of Comprehensive Income)

   Each of the above statements must have stamped "received" by the Bureau of Internal Revenue (BIR) or its duly accredited and authorized institutions.

<u>OR</u>

5. Submission of valid and current PHILGEPS Certificate of Registration and Membership (Platinum Registration) together with Annex A in lieu of the eligibility documents.

   Note: Bidder must ensure that all Class "A" Eligibility Documents are valid and current at the time of submission of PHILGEPS Certificate of Registration and Membership (Platinum Registration). In case any of the submitted Eligibility are not valid and current at the time of submission of Platinum Registration, bidders are required to submit the valid and current documents.

In case the JV Partners opt to submit their Class "A" Documents, the Certificate of PhilGEPS Registration (Platinum Membership) shall remain as post-qualification requirement to be submitted in accordance with Section 34.2 of the 2016 Revised IRR of RA9184. "GPPB Circular 07-2017 dated 31 July 2017".

For item (v) to (vi) of the required Eligibility Documents, submission by any of the Joint Venture **partner constitutes compliance.**

(b) **TECHNICAL DOCUMENTS –**

i. Bid security shall be issued in favor of the **DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT) valid at least one hundred twenty (120) calendar days after date of bid opening** in any of the following forms:

a) BID SECURING DECLARATION per **Annex IV;** or
b) Cashier's / Manager's Check equivalent to at least 2% of ABC issued by an Universal or Commercial Bank.
c) Bank Draft / Guarantee or Irrevocable Letter of Credit issued by a Universal or Commercial Bank equivalent to at least 2% of the ABC: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank
d) Surety Bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security equivalent to at least 5% of the ABC

Description		SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
Qty		1 Lot
Total ABC (VAT Inclusive)		PhP512,000,000.00
BID SECURITY	Cashier's / Manager's Check equivalent to at least 2% of the ABC	PhP10,240,000.00
	Bank Draft / Guarantee or Irrevocable Letter of Credit equivalent to at least 2 % of the ABC	PhP10,240,000.00

	Surety Bond equivalent to at least 5% of the ABC	PhP25,600,000.00
	Bid Securing Declaration	No required percentage

***NOTES:**

1. Should the bidder opt to submit Cashier's / Manager's Check as Bid Security, it must be issued by a Local Universal or Commercial Bank
2. Should the bidder opt to submit Bank Draft/Guarantee or Irrevocable Letter of Credit as Bid Security, it must be issued by a Local Universal or Local Commercial Bank
3. Should the bidder opt to submit a Surety Bond as Bid Security, the surety bond must conform with the following:
   a. Issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such bond. Together with the surety bond, a copy of a valid Certification from the Insurance Commission must be submitted by the bidder which must state that the surety or insurance company is specifically authorized to issue surety bond
   b. Callable upon demand
   c. Must expressly specify/indicate the grounds for forfeiture of bid security as state in Section II, ITB Clause 18.5, to wit:

      - If a Bidder:
        (i) Withdraws its bid during the period of bid validity specified in ITB Clause 17;
        (ii) Does not accept the correction of errors pursuant to ITB Clause 28.3(b);
        (iii) Has a finding against the veracity of any of the documents submitted as stated in ITB Clause 29.2;
        (iv) Submission of eligibility requirements containing false information or falsified documents;
        (v) Submits bids that contain false information or falsified documents, or the concealment of such information in the bids in order to influence the outcome of eligibility screening or any other stage of the public bidding;
        (vi) Allowing the use of one's name, or using the name of another for purposes of public bidding;
        (vii) Withdrawal of a bid, or refusal to accept an award, or enter into contract with the Government without justifiable cause, after the Bidder had been adjudged as having submitted the Lowest Calculated and Responsive Bid;
        (viii) Refusal or failure to post the required performance security within the prescribed time;

(ix) Refusal to clarify or validate in writing its bid during post-qualification within a period of seven (7) calendar days from receipt of the request for clarification;

(x) Any document attempted by a bidder to unduly influence the outcome of the bidding in his favor;

(xi) Failure of the potential joint venture partners to enter into joint venture after the bid is declared successful;

(xii) All other acts that tend to defeat the purpose of the competitive bidding such as habitually withdrawing from bidding, submitting late Bids or patently insufficient bid, for at least three (3) times within a year, except for valid reason.

- If the Successful Bidder:

(xiii) Fails to sign the contract in accordance with ITB Clause 32; or

(xiv) Fails to furnish performance security in accordance with ITB Clause 33

ii. Proof of Authority of the Bidder’s authorized representative/s:

a) FOR SOLE PROPRIETORSHIP (IF OWNER OPTS TO APPOINT A REPRESENTATIVE): Duly notarized Special Power of Attorney
b) FOR CORPORATIONS, COOPERATIVE OR THE MEMBERS OF THE JOINT VENTURE: Duly notarized Secretary’s Certificate evidencing the authority of the designated representative/s.
c) IN THE CASE OF UNINCORPORATED JOINT VENTURE: Each member shall submit a separate Special Power of Attorney and/or Secretary’s Certificate evidencing the authority of the designated representative/s.

iii. Omnibus Sworn Statements **(Annex V)**

a) Authority of the designated representative
b) Non-inclusion of blacklist or under suspension status
c) Authenticity of Submitted Documents
d) Authority to validate Submitted Documents
e) Disclosure of Relations
f) Compliance with existing labor laws and standards
g) Bidders Responsibilities
h) Did not pay any form of consideration
i) Company Official Contact Reference

iv. Company Profile **(Annex VI).** Company printed brochure may be included;

v. Vicinity / Location of Bidder’s principal place of business

***Note:** In case of Joint Venture, both partners must present copy of items iv. and v.

vi. Certificate of Performance Evaluation **(Annex VII)** showing a rating at least Satisfactory issued by the Bidder's Single Largest Completed Contract Client stated in the submitted Annex I-A;

vii. Completed and signed Technical Bid Form **(Annex VIII);**

viii. Business Registration Certificate (BRC) with a minimum of five (5) years of experience in the field of intelligence, threat detection and cyber security;

ix. Valid Certification from at least two (2) of the bidder's clients to prove that they have performed cyber forensic investigations specifically involving external attackers;

x. Bidder's portfolio or any documentary report to prove that they have deep intelligence in cyber threat actors especially those related to financial crimes and critical infrastructure;

xi. Product specification and/or datasheet to prove that it has the technology to scale the forensic assessment to all Windows systems;

xii. Product datasheet to prove expertise in the following:

a) Analysis of computer systems, network traffic transiting between customer's network and the Internet
b) Assessment of regular status report, assessment report of relevant findings, and recommendations for improvement and executive brief report
c) Executive-level briefing detailing necessary recommendations to improve incident preparedness capabilities
d) Computer security incident response support
e) Forensics, log and advanced malware analysis
f) Advanced threat actor response support
g) Advanced threat/incident remediation assistance

xiii. Technical Data Sheet or equivalent document for the following tools and services:

a) Threat Intelligence Platform
b) Web Intelligence Tool
c) Network Protection Tools
d) Next Generation Firewall (NGFW)
e) Distributed Denial of Service (DDos) Protection Tool

f) IPS/IDS
g) Application Delivery Controller (ADC)
h) Log Collection and Correlation Tool
i) Artificial Intelligence (AI) / Machine Learning
j) Portable CMS
k) Disaster Recovery Management System Tool
l) VAPT Tool

***Note:** If in foreign language other than English, it must be accompanied by a translation of the documents in English. The documents shall be translated by the relevant foreign government agency, the foreign government agency authorized to translate documents, or a registered translator in the foreign bidder's country, and shall be authenticated by the appropriate Philippine foreign service establishment/post or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines.

xiv. Valid and Current Certificate of Distributorship / Dealership/ Resellership of the following product being offered, issued by the principal or manufacturer of the product (if Bidder is not the manufacturer). If not issued by manufacturer, must also submit certification / document linking bidder to the manufacturer.

a) Web Intelligence Tool
b) Network Protection Tools
c) Next Generation Firewall (NGFW)
d) Distributed Denial of Service (DDos) Protection Tool
e) IPS/IDS
f) Application Delivery Controller (ADC)
g) Log Collection and Correlation Tool
h) Artificial Intelligence (AI) / Machine Learning
i) Portable CMS
j) Disaster Recovery Management System Tool
k) VAPT Tool

Note: If in foreign language other than English, it must be accompanied by a translation of the documents in English. The documents shall be translated by the relevant foreign government agency, the foreign government agency authorized to translate documents, or a registered translator in the foreign bidder's country, and shall be authenticated by the appropriate Philippine foreign service establishment/post or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. Threat Intelligence Platform

	xv. Compliance with the Schedule of Requirements **(Section VI);** and xvi. Compliance with the Technical Specifications **(Section VII)** xvii. For foreign bidders claiming eligibility by reason of their country's extension of reciprocal rights to Filipinos, a certification from the relevant government office of their country stating that Filipinos are allowed to participate in their government procurement activities for the same item or product.
13.1	The financial component of the bid shall contain the following: i. Completed and signed Financial Bid Form **(Annex IX)** ii. Completed and signed Detailed Financial Breakdown **(Annex X)** iii. Completed and signed form "For Goods Offered from Abroad" **(Annex XI-A)** and/or form "For Goods Offered from within the Philippines" **(Annex XI-B)**, whichever is applicable. The total ABC is inclusive of VAT. Any proposal with a financial component exceeding the ABC shall not be accepted. Bid for each item in the lot indicated in the Financial Bid Form (Annex IX) must be equal to the signed and submitted Detailed Financial Breakdown (Annex X). If the Supplier claims preference as a Domestic Supplier or Domestic Entity, a certification from the DTI, SEC, or CDA to be enclosed pursuant to the Revised IRR of RA 9184.
13.1(b)	No further instructions.
13.1(c)	Bid for each item in the lot indicated in the Detailed Financial Breakdown (Annex X), form "For Goods Offered from Abroad" (Annex XI-A) and/or form "For Goods Offered from within the Philippines" (Annex XI-B) must be equal to the signed submitted Financial Bid Form (Annex IX) and must not exceed the total ABC.
13.2	The ABC is **Five Hundred Twelve Million Pesos (PhP512,000,000.00).** Any bid with a financial component exceeding this amount shall not be accepted.
15.4(a)(iv)	No incidental services are required.
15.4(b)	No incidental services are required.
16.1(b)	The Bid prices for Goods supplied from outside of the Philippines shall be quoted in Philippine Pesos.
16.3	Not applicable.
17.1	Bids will be valid for one hundred twenty (120) calendar days after date of bid opening.

18.1

Bid security shall be issued in favor of the **DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT) valid at least one hundred twenty (120) calendar days after date of bid opening** in any of the following forms:

a) BID SECURING DECLARATION per **Annex IV;** or
b) Cashier's / Manager's Check equivalent to at least 2% of ABC issued by an Universal or Commercial Bank.
c) Bank Draft / Guarantee or Irrevocable Letter of Credit issued by a Universal or Commercial Bank equivalent to at least 2% of the ABC: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank
d) Surety Bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security equivalent to at least 5% of the ABC

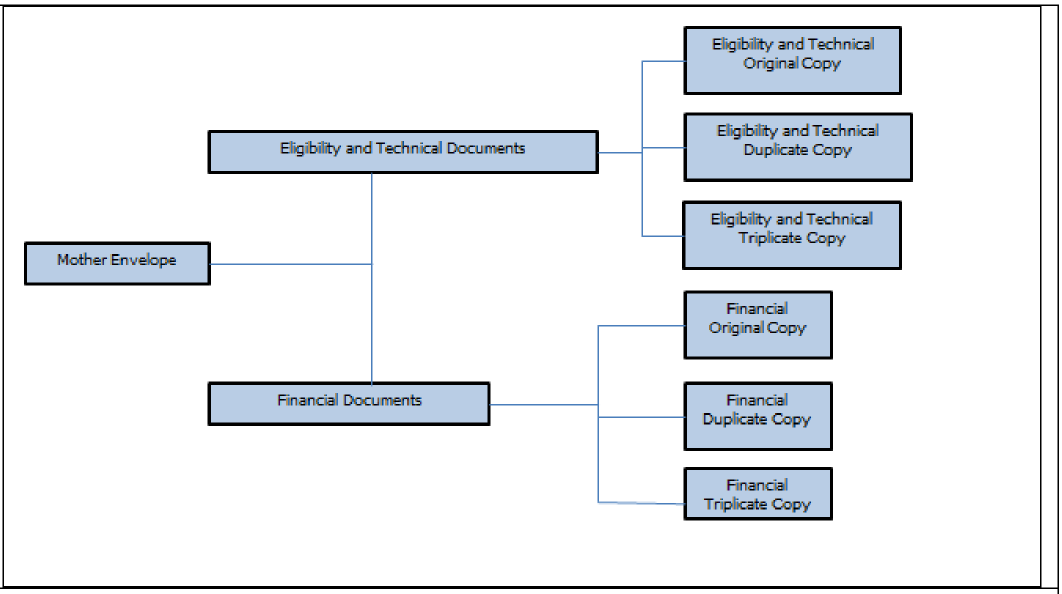
Description		**SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT**
Qty		1 Lot
Total ABC (VAT Inclusive)		PhP512,000,000.00
BID SECURITY	**Cashier's / Manager's Check equivalent to at least 2% of the ABC**	PhP10,240,000.00
	Bank Draft / Guarantee or Irrevocable Letter of Credit equivalent to at least 2 % of the ABC	PhP10,240,000.00
	Surety Bond equivalent to at least 5% of the ABC	PhP25,600,000.00
	Bid Securing Declaration	No required percentage

***NOTES:**

1. Should the bidder opt to submit Cashier's / Manager's Check as Bid Security, it must be issued by a Local Universal or Commercial Bank
2. Should the bidder opt to submit Bank Draft/Guarantee or Irrevocable Letter of Credit as Bid Security, it must be issued by a Local Universal or Local Commercial Bank
3. Should the bidder opt to submit a Surety Bond as Bid Security, the surety bond must conform with the following:
   a. Issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such bond. Together with the surety bond, a copy of a valid Certification from the Insurance Commission must be submitted by the bidder which must state that the surety or insurance company is specifically authorized to issue surety bond

	b. Callable upon demand c. Must expressly specify/indicate the grounds for forfeiture of bid security as state in Section II, ITB Clause 18.5, to wit: • If a Bidder: (i) Withdraws its bid during the period of bid validity specified in ITB Clause 17; (ii) Does not accept the correction of errors pursuant to ITB Clause 28.3(b); (iii) Has a finding against the veracity of any of the documents submitted as stated in ITB Clause 29.2; (iv) Submission of eligibility requirements containing false information or falsified documents; (v) Submits bids that contain false information or falsified documents, or the concealment of such information in the bids in order to influence the outcome of eligibility screening or any other stage of the public bidding; (vi) Allowing the use of one's name, or using the name of another for purposes of public bidding; (vii) Withdrawal of a bid, or refusal to accept an award, or enter into contract with the Government without justifiable cause, after the Bidder had been adjudged as having submitted the Lowest Calculated and Responsive Bid; (viii) Refusal or failure to post the required performance security within the prescribed time; (ix) Refusal to clarify or validate in writing its bid during post-qualification within a period of seven (7) calendar days from receipt of the request for clarification; (x) Any document attempted by a bidder to unduly influence the outcome of the bidding in his favor; (xi) Failure of the potential joint venture partners to enter into joint venture after the bid is declared successful; (xii) All other acts that tend to defeat the purpose of the competitive bidding such as habitually withdrawing from bidding, submitting late Bids or patently insufficient bid, for at least three (3) times within a year, except for valid reason. • If the Successful Bidder: (xiii) Fails to sign the contract in accordance with ITB Clause 32; or (xiv) Fails to furnish performance security in accordance with ITB Clause 33
18.2	The bid security shall be valid for one hundred twenty (120) calendar days from the date of opening of bids.

<table>
<tr>
<td>20.3</td>
<td>
<p>Each Bidder shall submit one (1) original and two (2) copies of the first and second components of its bid.</p>
<p>First envelope must contain three (3) copies of Eligibility and Technical documents duly marked as “Original Copy”, “Duplicate Copy”, and “Triplicate Copy”.</p>
<p>Second envelope must contain three (3) copies of Financial documents duly marked as “Original Copy”, “Duplicate Copy”, and “Triplicate Copy”.</p>
<p>All envelopes shall:</p>
<p>a) Contain the name of the contract to be bid in capital letters;</p>
<p>b) Bear the name and address of the Bidder in capital letters;</p>
<p>c) Be addressed to the Procuring Entity’s BAC in accordance with <b>ITB Clause 1.1</b>;</p>
<p>d) Bear the specific identification of this bidding process indicated in the ITB Clause 1.2; and</p>
<p>e) Bear a warning “DO NO OPEN BEFORE…” the date and time for the opening of bids, in accordance with <b>ITB Clause 21</b>.</p>
<table>
<tr><td>TO</td><td>: <b>DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY</b></td></tr>
<tr><td>FROM</td><td>: ________________________________
(Name of Bidder in Capital Letters)</td></tr>
<tr><td>ADDRESS</td><td>: ________________________________
(Address of Bidder in Capital Letters)</td></tr>
<tr><td>PROJECT</td><td>: <b>SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT</b></td></tr>
<tr><td>BID REF NO</td><td><b>: BAC4G&S-2018-002</b></td></tr>
<tr><td colspan="2">(In Capital Letters, Indicate the Phrase):
“DO NOT OPEN BEFORE: 25 JUNE 2018, 1:30PM<b>”</b></td></tr>
</table>
</td>
</tr>
</table>

	 Mother Envelope Eligibility and Technical Documents Eligibility and Technical Original Copy Eligibility and Technical Duplicate Copy Eligibility and Technical Triplicate Copy Financial Documents Financial Original Copy Financial Duplicate Copy Financial Triplicate Copy
21	The address for submission of bids is **Department of Information and Communications Technology Building, C.P. Garcia Avenue, Diliman, Quezon City** The **Deadline for Submission of Bids** is **25 June 2018, 12 Noon.**
24.1	The place of bid opening is **Executive Lounge, Lower Ground Floor, Department of Information and Communications Technology Building, C.P. Garcia Avenue, Diliman, Quezon City.** The **date and time of Bid Opening** is on **25 June 2018, 1:30PM.**
24.2	No further instructions.
24.3	No further instructions.
27.1	No further instructions.
28.3 (a)	**Grouping and Evaluation of Lots** All items to be grouped together to form one complete Lot that will be awarded to one Bidder to form one complete contract. Partial bid is not allowed. The goods are grouped in a single lot and the lot shall not be divided into sub-lots for the purpose of bidding, evaluation, and contract award. In all cases, the NFCC computation, if applicable, must be sufficient for all the lots or contracts to be awarded to the Bidder.
28.4	No further instructions.
29.2	**Post Qualification:** Within a non-extendible period of five (5) calendar days from receipt by the Supplier of the Notice from the BAC that the supplier has the Single/Lowest Calculated Bid (S/LCB), the Supplier shall submit the requirement for post qualification:

	● Latest Income Tax Returns per Revenue Regulations 3-2005 Tax returns or tax returns filed through the Electronic Filing and Payments System (EFPS). The latest income and business tax returns are those within the last six months preceding the date of bid submission; (including VAT Returns and its corresponding proof of payment) ***In Case of Joint Venture, both partners must present/submit above item.** Failure of the bidder, declared as Single/Lowest Calculated Bid (S/LCB), to duly submit the above requirements or a finding against the veracity of such shall be ground for forfeiture of the bid security of the IRR of RA 9184. As part of Post Qualification, eligibility and technical documents submitted by the S/LCB will be validated and verified. Furthermore, S/LCB product technical specifications will be validated to ensure compliance with the required specifications.
32.4(f)	No additional requirement.

Section IV.
General Condition of Contract

1. Definitions

1.1. In this Contract, the following terms shall be interpreted as indicated:

(a) "The Contract" means the agreement entered into between the Procuring Entity and the Supplier, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

(b) "The Contract Price" means the price payable to the Supplier under the Contract for the full and proper performance of its contractual obligations.

(c) "The Goods" means all of the supplies, equipment, machinery, spare parts, other materials and/or general support services which the Supplier is required to provide to the Procuring Entity under the Contract.

(d) "The Services" means those services ancillary to the supply of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training, and other such obligations of the Supplier covered under the Contract.

(e) "GCC" means the General Conditions of Contract contained in this Section.

(f) "SCC" means the Special Conditions of Contract.

(g) "The Procuring Entity" means the organization purchasing the Goods, as named in the **SCC**.

(h) "The Procuring Entity's country" is the Philippines.

(i) "The Supplier" means the individual contractor, manufacturer distributor, or firm supplying/manufacturing the Goods and Services under this Contract and named in the **SCC**.

(j) The "Funding Source" means the organization named in the **SCC**.

(k) "The Project Site," where applicable, means the place or places named in the **SCC**.

(l) "Day" means calendar day.

(m) The "Effective Date" of the contract will be the date of signing the contract, however the Supplier shall commence performance of its obligations only upon receipt of the Notice to Proceed and copy of the approved contract.

(n) "Verified Report" refers to the report submitted by the Implementing Unit to the HoPE setting forth its findings as to the existence of grounds or causes for termination and explicitly stating its recommendation for the issuance of a Notice to Terminate.

2. Corrupt, Fraudulent, Collusive, and Coercive Practices

2.1. Unless otherwise provided in the **SCC**, the Procuring Entity as well as the bidders, contractors, or suppliers shall observe the highest standard of ethics during the procurement and execution of this Contract. In pursuance of this policy, the Procuring Entity:

(a) defines, for the purposes of this provision, the terms set forth below as follows:

(i) "corrupt practice" means behavior on the part of officials in the public or private sectors by which they improperly and unlawfully enrich themselves, others, or induce others to do so, by misusing the position in which they are placed, and it includes the offering, giving, receiving, or soliciting of anything of value to influence the action of any such official in the procurement process or in contract execution; entering, on behalf of the Government, into any contract or transaction manifestly and grossly disadvantageous to the same, whether or not the public officer profited or will profit thereby, and similar acts as provided in Republic Act 3019.

(ii) "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Procuring Entity, and includes collusive practices among Bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the Procuring Entity of the benefits of free and open competition.

(iii) "collusive practices" means a scheme or arrangement between two or more Bidders, with or without the knowledge of the Procuring Entity, designed to establish bid prices at artificial, non-competitive levels.

(iv) "coercive practices" means harming or threatening to harm, directly or indirectly, persons, or their property to influence their participation in a procurement process, or affect the execution of a contract;

(v) "obstructive practice" is

(aa) deliberately destroying, falsifying, altering or concealing of evidence material to an administrative proceedings or investigation or making false statements to investigators in order to materially impede an administrative proceedings or investigation of the Procuring Entity or any foreign government/foreign or international financing institution into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the administrative proceedings or investigation or from pursuing such proceedings or investigation; or

(bb) acts intended to materially impede the exercise of the inspection and audit rights of the Procuring Entity or any foreign government/foreign or international financing institution herein.

(b) will reject a proposal for award if it determines that the Bidder recommended for award has engaged in any of the practices mentioned in this Clause for purposes of competing for the contract.

2.2. Further the Funding Source, Borrower or Procuring Entity, as appropriate, will seek to impose the maximum civil, administrative and/or criminal penalties available under the applicable law on individuals and organizations deemed to be involved with any of the practices mentioned in **GCC** Clause 2.1(a).

3. Inspection and Audit by the Funding Source

The Supplier shall permit the Funding Source to inspect the Supplier's accounts and records relating to the performance of the Supplier and to have them audited by auditors appointed by the Funding Source, if so required by the Funding Source.

4. Governing Law and Language

4.1. This Contract shall be interpreted in accordance with the laws of the Republic of the Philippines.

4.2. This Contract has been executed in the English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract. All correspondence and other documents pertaining to this Contract exchanged by the parties shall be written in English.

5. Notices

5.1. Any notice, request, or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request, or consent shall be deemed to have been given or made when received by the concerned party, either in person or through an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram, or facsimile to such Party at the address specified in the **SCC**, which shall be effective when delivered and duly received or on the notice's effective date, whichever is later.

5.2. A Party may change its address for notice hereunder by giving the other Party notice of such change pursuant to the provisions listed in the **SCC** for **GCC** Clause 5.1.

6. Scope of Contract

6.1. The Goods and Related Services to be provided shall be as specified in Section VI. Schedule of Requirements.

6.2. This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. Any additional requirements for the completion of this Contract shall be provided in the **SCC**.

7. Subcontracting

7.1. Subcontracting of any portion of the Goods, if allowed in the **BDS**, does not relieve the Supplier of any liability or obligation under this Contract. The

Supplier will be responsible for the acts, defaults, and negligence of any subcontractor, its agents, servants or workmen as fully as if these were the Supplier's own acts, defaults, or negligence, or those of its agents, servants or workmen.

7.2. If subcontracting is allowed, the Supplier may identify its subcontractor during contract implementation. Subcontractors disclosed and identified during the bidding may be changed during the implementation of this Contract. In either case, subcontractors must submit the documentary requirements under **ITB** Clause 12 and comply with the eligibility criteria specified in the **BDS.** In the event that any subcontractor is found by the Procuring Entity to be ineligible, the subcontracting of such portion of the Goods shall be disallowed.

8. Procuring Entity's Responsibilities

8.1. Whenever the performance of the obligations in this Contract requires that the Supplier obtain permits, approvals, import, and other licenses from local public authorities, the Procuring Entity shall, if so needed by the Supplier, make its best effort to assist the Supplier in complying with such requirements in a timely and expeditious manner.

8.2. The Procuring Entity shall pay all costs involved in the performance of its responsibilities in accordance with **GCC** Clause 6.

9. Prices

9.1. For the given scope of work in this Contract as awarded, all bid prices are considered fixed prices, and therefore not subject to price escalation during contract implementation, except under extraordinary circumstances and upon prior approval of the GPPB in accordance with Section 61 of R.A. 9184 and its IRR or except as provided in this Clause.

9.2. Prices charged by the Supplier for Goods delivered and/or services performed under this Contract shall not vary from the prices quoted by the Supplier in its bid, with the exception of any change in price resulting from a Change Order issued in accordance with **GCC** Clause 29.

10. Payment

10.1. Payments shall be made only upon a certification by the HoPE to the effect that the Goods have been rendered or delivered in accordance with the terms of this Contract and have been duly inspected and accepted**.** Except with the prior approval of the President no payment shall be made for services not yet rendered or for supplies and materials not yet delivered under this Contract. Ten percent (10%) of the amount of each payment shall be retained by the Procuring Entity to cover the Supplier's warranty obligations under this Contract as described in **GCC** Clause 17.

10.2. The Supplier's request(s) for payment shall be made to the Procuring Entity in writing, accompanied by an invoice describing, as appropriate, the Goods delivered and/or Services performed, and by documents submitted pursuant to the **SCC** provision for **GCC** Clause 6.2, and upon fulfillment of other obligations stipulated in this Contract.

10.3. Pursuant to **GCC** Clause 10.2, payments shall be made promptly by the Procuring Entity, but in no case later than sixty (60) days after submission of an invoice or claim by the Supplier. Payments shall be in accordance with the schedule stated in the **SCC**.

10.4. Unless otherwise provided in the **SCC**, the currency in which payment is made to the Supplier under this Contract shall be in Philippine Pesos.

10.5. Unless otherwise provided in the **SCC**, payments using Letter of Credit (LC), in accordance with the Guidelines issued by the GPPB, is allowed. For this purpose, the amount of provisional sum is indicated in the **SCC**. All charges for the opening of the LC and/or incidental expenses thereto shall be for the account of the Supplier.

11. Advance Payment and Terms of Payment

11.1. Advance payment shall be made only after prior approval of the President, and shall not exceed fifteen percent (15%) of the Contract amount, unless otherwise directed by the President or in cases allowed under Annex "D" of RA 9184.

11.2. All progress payments shall first be charged against the advance payment until the latter has been fully exhausted.

11.3. For Goods supplied from abroad, unless otherwise indicated in the **SCC**, the terms of payment shall be as follows:

(a) On Contract Signature: Fifteen Percent (15%) of the Contract Price shall be paid within sixty (60) days from signing of the Contract and upon submission of a claim and a bank guarantee for the equivalent amount valid until the Goods are delivered and in the form provided in Section VIII. Bidding Forms.

(b) On Delivery: Sixty-five percent (65%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of receipt of the Goods and upon submission of the documents (i) through (vi) specified in the SCC provision on Delivery and Documents.

(c) On Acceptance: The remaining twenty percent (20%) of the Contract Price shall be paid to the Supplier within sixty (60) days after the date of submission of the acceptance and inspection certificate for the respective delivery issued by the Procuring Entity's authorized representative. In the event that no inspection or acceptance certificate is issued by the Procuring Entity's authorized representative within forty five (45) days of the date shown on the delivery receipt, the Supplier shall have the right to claim payment of the remaining twenty percent (20%) subject to the Procuring Entity's own verification of the reason(s) for the failure to issue documents (vii) and (viii) as described in the SCC provision on Delivery and Documents.

12. Taxes and Duties

The Supplier, whether local or foreign, shall be entirely responsible for all the necessary taxes, stamp duties, license fees, and other such levies imposed for the completion of this Contract.

13. Performance Security

13.1. Within ten (10) calendar days from receipt of the Notice of Award from the Procuring Entity but in no case later than the signing of the contract by both parties, the successful Bidder shall furnish the performance security in any the forms prescribed in the **ITB** Clause 33.2.

13.2. The performance security posted in favor of the Procuring Entity shall be forfeited in the event it is established that the winning bidder is in default in any of its obligations under the contract.

13.3. The performance security shall remain valid until issuance by the Procuring Entity of the Certificate of Final Acceptance.

13.4. The performance security may be released by the Procuring Entity and returned to the Supplier after the issuance of the Certificate of Final Acceptance subject to the following conditions:

(a) There are no pending claims against the Supplier or the surety company filed by the Procuring Entity;

(b) The Supplier has no pending claims for labor and materials filed against it; and

(c) Other terms specified in the **SCC**.

13.5. In case of a reduction of the contract value, the Procuring Entity shall allow a proportional reduction in the original performance security, provided that any such reduction is more than ten percent (10%) and that the aggregate of such reductions is not more than fifty percent (50%) of the original performance security.

14. Use of Contract Documents and Information

14.1. The Supplier shall not, except for purposes of performing the obligations in this Contract, without the Procuring Entity's prior written consent, disclose this Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the Procuring Entity. Any such disclosure shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.

14.2. Any document, other than this Contract itself, enumerated in **GCC** Clause 14.1 shall remain the property of the Procuring Entity and shall be returned (all copies) to the Procuring Entity on completion of the Supplier's performance under this Contract if so required by the Procuring Entity.

15. Standards

The Goods provided under this Contract shall conform to the standards mentioned in the Section VII. Technical Specifications; and, when no applicable standard is mentioned, to the authoritative standards appropriate to the Goods' country of origin. Such standards shall be the latest issued by the institution concerned.

16. Inspection and Tests

16.1. The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Contract specifications at no extra cost to the Procuring Entity. The **SCC** and Section VII. Technical Specifications shall specify what inspections and/or tests the Procuring Entity requires and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

16.2. If applicable, the inspections and tests may be conducted on the premises of the Supplier or its subcontractor(s), at point of delivery, and/or at the goods' final destination. If conducted on the premises of the Supplier or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Procuring Entity. The Supplier shall provide the Procuring Entity with results of such inspections and tests.

16.3. The Procuring Entity or its designated representative shall be entitled to attend the tests and/or inspections referred to in this Clause provided that the Procuring Entity shall bear all of its own costs and expenses incurred in connection with such attendance including, but not limited to, all traveling and board and lodging expenses.

16.4. The Procuring Entity may reject any Goods or any part thereof that fail to pass any test and/or inspection or do not conform to the specifications. The Supplier shall either rectify or replace such rejected Goods or parts thereof or make alterations necessary to meet the specifications at no cost to the Procuring Entity, and shall repeat the test and/or inspection, at no cost to the Procuring Entity, upon giving a notice pursuant to **GCC** Clause 5.

16.5. The Supplier agrees that neither the execution of a test and/or inspection of the Goods or any part thereof, nor the attendance by the Procuring Entity or its representative, shall release the Supplier from any warranties or other obligations under this Contract.

17. Warranty

17.1. The Supplier warrants that the Goods supplied under the Contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials, except when the technical specifications required by the Procuring Entity provides otherwise.

17.2. The Supplier further warrants that all Goods supplied under this Contract shall have no defect, arising from design, materials, or workmanship or from any act or omission of the Supplier that may develop under normal use of the supplied Goods in the conditions prevailing in the country of final destination.

17.3. In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier for a minimum period specified in the **SCC**. The obligation for the warranty shall be covered by, at the Supplier's option, either retention money in an amount equivalent to at least one percent (1%) of every progress payment, or a special bank guarantee equivalent to at least one percent (1%) of the total Contract Price or other such amount if so specified in the **SCC**. The said amounts shall only be released after the lapse of the warranty period specified in the **SCC**; provided, however, that the Supplies delivered are free from patent and latent defects and all the conditions imposed under this Contract have been fully met.

17.4. The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, within the period specified in the **SCC** and with all reasonable speed, repair or replace the defective Goods or parts thereof, without cost to the Procuring Entity.

17.5. If the Supplier, having been notified, fails to remedy the defect(s) within the period specified in **GCC** Clause 17.4, the Procuring Entity may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights which the Procuring Entity may have against the Supplier under the Contract and under the applicable law.

18. Delays in the Supplier's Performance

18.1. Delivery of the Goods and/or performance of Services shall be made by the Supplier in accordance with the time schedule prescribed by the Procuring Entity in Section VI. Schedule of Requirements.

18.2. If at any time during the performance of this Contract, the Supplier or its Subcontractor(s) should encounter conditions impeding timely delivery of the Goods and/or performance of Services, the Supplier shall promptly notify the Procuring Entity in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Supplier's notice, and upon causes provided for under **GCC** Clause 22, the Procuring Entity shall evaluate the situation and may extend the Supplier's time for performance, in which case the extension shall be ratified by the parties by amendment of Contract.

18.3. Except as provided under **GCC** Clause 22, a delay by the Supplier in the performance of its obligations shall render the Supplier liable to the imposition of liquidated damages pursuant to **GCC** Clause 19, unless an extension of time is agreed upon pursuant to **GCC** Clause 29 without the application of liquidated damages.

19. Liquidated Damages

Subject to **GCC** Clauses 18 and 22, if the Supplier fails to satisfactorily deliver any or all of the Goods and/or to perform the Services within the period(s) specified in this Contract inclusive of duly granted time extensions if any, the Procuring Entity shall, without prejudice to its other remedies under this Contract and under the applicable law, deduct from the Contract Price, as liquidated damages, the applicable rate of one tenth (1/10) of one (1) percent of the cost of the unperformed portion for every day of delay until actual delivery or performance. The maximum deduction shall be ten percent (10%) of the amount of contract. Once the maximum is reached, the Procuring Entity may rescind or terminate the Contract pursuant to **GCC** Clause 23, without prejudice to other courses of action and remedies open to it.

20. Settlement of Disputes

20.1. If any dispute or difference of any kind whatsoever shall arise between the Procuring Entity and the Supplier in connection with or arising out of this Contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

20.2. If after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the Procuring Entity or the

Supplier may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

20.3. Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this Clause shall be settled by arbitration. Arbitration may be commenced prior to or after delivery of the Goods under this Contract.

20.4. In the case of a dispute between the Procuring Entity and the Supplier, the dispute shall be resolved in accordance with Republic Act 9285 ("R.A. 9285"), otherwise known as the "Alternative Dispute Resolution Act of 2004."

20.5. Notwithstanding any reference to arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree; and the Procuring Entity shall pay the Supplier any monies due the Supplier.

21. Liability of the Supplier

21.1. The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines, subject to additional provisions, if any, set forth in the **SCC**.

21.2. Except in cases of criminal negligence or willful misconduct, and in the case of infringement of patent rights, if applicable, the aggregate liability of the Supplier to the Procuring Entity shall not exceed the total Contract Price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

22. Force Majeure

22.1. The Supplier shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default if and to the extent that the Supplier's delay in performance or other failure to perform its obligations under the Contract is the result of a *force majeure*.

22.2. For purposes of this Contract the terms "*force majeure*" and "fortuitous event" may be used interchangeably. In this regard, a fortuitous event or *force majeure* shall be interpreted to mean an event which the Supplier could not have foreseen, or which though foreseen, was inevitable. It shall not include ordinary unfavorable weather conditions; and any other cause the effects of which could have been avoided with the exercise of reasonable diligence by the Supplier. Such events may include, but not limited to, acts of the Procuring Entity in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.

22.3. If a *force majeure* situation arises, the Supplier shall promptly notify the Procuring Entity in writing of such condition and the cause thereof. Unless otherwise directed by the Procuring Entity in writing, the Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the *force majeure*.

23. Termination for Default

23.1. The Procuring Entity shall terminate this Contract for default when any of the following conditions attends its implementation:

(a) Outside of *force majeure*, the Supplier fails to deliver or perform any or all of the Goods within the period(s) specified in the contract, or within any extension thereof granted by the Procuring Entity pursuant to a request made by the Supplier prior to the delay, and such failure amounts to at least ten percent (10%) of the contact price;

(b) As a result of *force majeure*, the Supplier is unable to deliver or perform any or all of the Goods, amounting to at least ten percent (10%) of the contract price, for a period of not less than sixty (60) calendar days after receipt of the notice from the Procuring Entity stating that the circumstance of force majeure is deemed to have ceased; or

(c) The Supplier fails to perform any other obligation under the Contract.

23.2. In the event the Procuring Entity terminates this Contract in whole or in part, for any of the reasons provided under **GCC** Clauses 23 to 26, the Procuring Entity may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Supplier shall be liable to the Procuring Entity for any excess costs for such similar Goods or Services. However, the Supplier shall continue performance of this Contract to the extent not terminated.

23.3. In case the delay in the delivery of the Goods and/or performance of the Services exceeds a time duration equivalent to ten percent (10%) of the specified contract time plus any time extension duly granted to the Supplier, the Procuring Entity may terminate this Contract, forfeit the Supplier's performance security and award the same to a qualified Supplier.

24. Termination for Insolvency

The Procuring Entity shall terminate this Contract if the Supplier is declared bankrupt or insolvent as determined with finality by a court of competent jurisdiction. In this event, termination will be without compensation to the Supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Procuring Entity and/or the Supplier.

25. Termination for Convenience

25.1. The Procuring Entity may terminate this Contract, in whole or in part, at any time for its convenience. The HoPE may terminate a contract for the convenience of the Government if he has determined the existence of conditions that make Project Implementation economically, financially or technically impractical and/or unnecessary, such as, but not limited to, fortuitous event(s) or changes in law and national government policies.

25.2. The Goods that have been delivered and/or performed or are ready for delivery or performance within thirty (30) calendar days after the Supplier's receipt of Notice to Terminate shall be accepted by the Procuring Entity at the contract terms and prices. For Goods not yet performed and/or ready for delivery, the Procuring Entity may elect:

(a) to have any portion delivered and/or performed and paid at the contract terms and prices; and/or

(b) to cancel the remainder and pay to the Supplier an agreed amount for partially completed and/or performed goods and for materials and parts previously procured by the Supplier.

25.3. If the Supplier suffers loss in its initial performance of the terminated contract, such as purchase of raw materials for goods specially manufactured for the Procuring Entity which cannot be sold in open market, it shall be allowed to recover partially from this Contract, on a *quantum meruit* basis. Before recovery may be made, the fact of loss must be established under oath by the Supplier to the satisfaction of the Procuring Entity before recovery may be made.

26. Termination for Unlawful Acts

26.1. The Procuring Entity may terminate this Contract in case it is determined *prima facie* that the Supplier has engaged, before or during the implementation of this Contract, in unlawful deeds and behaviors relative to contract acquisition and implementation. Unlawful acts include, but are not limited to, the following:

(a) Corrupt, fraudulent, and coercive practices as defined in **ITB** Clause 3.1(a);

(b) Drawing up or using forged documents;

(c) Using adulterated materials, means or methods, or engaging in production contrary to rules of science or the trade; and

(d) Any other act analogous to the foregoing.

27. Procedures for Termination of Contracts

27.1. The following provisions shall govern the procedures for termination of this Contract:

(a) Upon receipt of a written report of acts or causes which may constitute ground(s) for termination as aforementioned, or upon its own initiative, the Implementing Unit shall, within a period of seven (7) calendar days, verify the existence of such ground(s) and cause the execution of a Verified Report, with all relevant evidence attached;

(b) Upon recommendation by the Implementing Unit, the HoPE shall terminate this Contract only by a written notice to the Supplier conveying the termination of this Contract. The notice shall state:

(i) that this Contract is being terminated for any of the ground(s) afore-mentioned, and a statement of the acts that constitute the ground(s) constituting the same;

(ii) the extent of termination, whether in whole or in part;

(iii) an instruction to the Supplier to show cause as to why this Contract should not be terminated; and

(iv) special instructions of the Procuring Entity, if any.

(c) The Notice to Terminate shall be accompanied by a copy of the Verified Report;

(d) Within a period of seven (7) calendar days from receipt of the Notice of Termination, the Supplier shall submit to the HoPE a verified position paper stating why this Contract should not be terminated. If the Supplier fails to show cause after the lapse of the seven (7) day period, either by inaction or by default, the HoPE shall issue an order terminating this Contract;

(e) The Procuring Entity may, at any time before receipt of the Supplier's verified position paper described in item (d) above withdraw the Notice to Terminate if it is determined that certain items or works subject of the notice had been completed, delivered, or performed before the Supplier's receipt of the notice;

(f) Within a non-extendible period of ten (10) calendar days from receipt of the verified position paper, the HoPE shall decide whether or not to terminate this Contract. It shall serve a written notice to the Supplier of its decision and, unless otherwise provided, this Contract is deemed terminated from receipt of the Supplier of the notice of decision. The termination shall only be based on the ground(s) stated in the Notice to Terminate;

(g) The HoPE may create a Contract Termination Review Committee (CTRC) to assist him in the discharge of this function. All decisions recommended by the CTRC shall be subject to the approval of the HoPE; and

(h) The Supplier must serve a written notice to the Procuring Entity of its intention to terminate the contract at least thirty (30) calendar days before its intended termination. The Contract is deemed terminated if it is not resumed in thirty (30) calendar days after the receipt of such notice by the Procuring Entity.

28. Assignment of Rights

The Supplier shall not assign his rights or obligations under this Contract, in whole or in part, except with the Procuring Entity's prior written consent.

29. Contract Amendment

Subject to applicable laws, no variation in or modification of the terms of this Contract shall be made except by written amendment signed by the parties.

30. Application

These General Conditions shall apply to the extent that they are not superseded by provisions of other parts of this Contract.

Section V.
Special Conditions of Contract (SCC)

Special Conditions of Contract

GCC Clause	
1.1(g)	The Procuring Entity is **DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT).**
1.1(i)	The Supplier is *[to be inserted at the time of contract award].*
1.1(j)	The Funding Source is from **the Government of the Philippines (GOP)** through **2018 GAA** in the amount of Pesos: **Five Hundred Twelve Million Pesos (PhP512,000,000.00)**
1.1(k)	The Project Site is at the Department of Information and Communications Technology (DICT), 49 Don A. Roces Ave, Quezon City
2.1	No further instructions.
5.1	The Procuring Entity's addressee, address and contact person for Notices is: **ELISEO M. RIO, JR.** **Acting Secretary** Department of Information and Communications Technology DICT Building, C.P. Garcia Avenue, Diliman, Quezon City Telephone No.: +63-02-9200101 **Contact Person** **ALLAN S. CABANLONG** Assistant Secretary for Cybersecurity and Enabling Technologies Department of Information and Communications Technology C.P. Garcia Avenue, Diliman, Quezon City Tel. No. +63-2-9200101 local 1002 Email Address: allan.cabanlong@dict.gov.ph Website: www.dict.gov.ph
6.2	**Delivery and Documents –** For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: *For Goods Supplied from Abroad, state* "The delivery terms applicable to the Contract are DDP delivered to the Department of Information and Communications Technology (DICT) at 49 Don A. Roces Ave, Diliman, Quezon City. In accordance with INCOTERMS."

For Goods Supplied from Within the Philippines, state "The delivery terms applicable to this Contract are delivered to the Department of Information and Communications Technology (DICT) at 49 Don A. Roces Ave, Diliman, Quezon City*.* Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination.”

Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI. Schedule of Requirements. The details of shipping and/or other documents to be furnished by the Supplier are as follows:

For Goods supplied from within the Philippines:

Upon delivery of the Goods to the Project Site, the Supplier shall notify the Procuring Entity and present the following documents to the Procuring Entity:

(i) Original and four copies of the Supplier’s invoice showing Goods’ description, quantity, unit price, and total amount;

(ii) Original and four copies delivery receipt/note, railway receipt, or truck receipt;

(iii) Original Supplier’s factory inspection report;

(iv) Original and four copies of the Manufacturer’s and/or Supplier’s warranty certificate;

(v) Original and four copies of the certificate of origin (for imported Goods);

(vi) Delivery receipt detailing number and description of items received signed by the authorized receiving personnel;

(vii) Certificate of Acceptance/Inspection Report signed by the Procuring Entity’s representative at the Project Site; and

(viii) Four copies of the Invoice Receipt for Property signed by the Procuring Entity’s representative at the Project Site.

For Goods supplied from abroad:

Upon shipment, the Supplier shall notify the Procuring Entity and the insurance company by cable the full details of the shipment, including Contract Number, description of the Goods, quantity, vessel, bill of lading number and date, port of loading, date of shipment, port of discharge etc. Upon delivery to the Project Site, the Supplier shall notify the Procuring Entity and present the following documents as applicable with the documentary requirements of any letter of credit issued taking precedence:

(i) Original and four copies of the Supplier's invoice showing Goods' description, quantity, unit price, and total amount;

(ii) Original and four copies of the negotiable, clean shipped on board bill of lading marked "freight pre-paid" and five copies of the non-negotiable bill of lading;

(iii) Original Supplier's factory inspection report;

(iv) Original and four copies of the Manufacturer's and/or Supplier's warranty certificate;

(v) Original and four copies of the certificate of origin (for imported Goods);

(vi) Delivery receipt detailing number and description of items received signed by the Procuring Entity's representative at the Project Site;

(vii) Certificate of Acceptance/Inspection Report signed by the Procuring Entity's representative at the Project Site; and

(viii) Four copies of the Invoice Receipt for Property signed by the Procuring Entity's representative at the Project Site.

For purposes of this Clause the Procuring Entity's Representative at the Project Site is Assistant Secretary Allan S. Cabanlong

Incidental Services –

The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements:

(a) performance or supervision of on-site assembly and/or startup of the supplied Goods;

(b) furnishing of tools required for assembly and/or maintenance of the supplied Goods;

(c) furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods;

(d) performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract; and

(e) Training of the Procuring Entity's personnel, at the Supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods.

The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.

Spare Parts –

The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier:

(a) such spare parts as the Procuring Entity may elect to purchase from the Supplier, provided that this election shall not relieve the Supplier of any warranty obligations under this Contract; and

(b) in the event of termination of production of the spare parts:

i. advance notification to the Procuring Entity of the pending termination, in sufficient time to permit the Procuring Entity to procure needed requirements; and

ii. following such termination, furnishing at no cost to the Procuring Entity, the blueprints, drawings, and specifications of the spare parts, if requested.

The spare parts required are listed in **Section VI. Schedule of Requirements** and the cost thereof are included in the Contract Price

Other spare parts and components shall be supplied as promptly as possible, but in any case within fifteen (15) days of placing the order.

Packaging –

The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the GOODS' final destination and the absence of heavy handling facilities at all points in transit.

The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity.

The outer packaging must be clearly marked on at least four (4) sides as follows:

Name of the Procuring Entity

Name of the Supplier

Contract Description

Final Destination

Gross weight

Any special lifting instructions

Any special handling instructions

Any relevant HAZCHEM classifications

A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging.

Insurance –

The Goods supplied under this Contract shall be fully insured by the Supplier in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage, and delivery. The Goods remain at the risk and title of the Supplier until their final acceptance by the Procuring Entity.

Transportation –

Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price.

Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the Contract Price.

Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when

	the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered *force majeure* in accordance with **GCC** Clause 22. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP Deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. **Patent Rights –** The Supplier shall indemnify the Procuring Entity against all thirdparty claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
10.4	Not applicable.
10.5	Payment using LC is not allowed.
11.3	Maintain the GCC Clause.
13.4(c)	No further instructions.
16.1	The inspections and tests that will be conducted are as stated in Section VII. Technical Specifications.
17.3	Two (2) years after acceptance by the Procuring Entity of the delivered Goods.
17.4	The period for correction of defects in the warranty period is fifteen (15) days.
21.1	No additional provision, however, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

Section VI.
Schedule of Requirements

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT

BAC4G&S-2018-002

Schedule of Requirement

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site

Description	Delivered, Weeks/Months
Hardware/Software Onsite Delivery	1 Month
Installation and configuration	0.5 Month
Testing and Submission of Testing Results & Documentations	0.5 Month
CMS Network VAPT	0.5 Month
Hardware/Software Delivery to Priority Agencies	2 Months
Installation and Configuration of Hardware/Software to Priority Agencies	2 Months
Operational Stress Test	0.5 Month
Knowledge Transfer	3 Months
TOTAL	**10 Months**

I hereby commit to comply and deliver all the above requirements in accordance with the above-stated schedule.

Name of Company	Signature Over Printed Name Of Authorized Representative	Date

Section VII.
Technical Specifications

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT

BAC4G&S-2018-002

TECHNICAL SPECIFICATIONS

Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of **ITB** Clause 3.1.(a)(ii) and/or **GCC** Clause 2.1(a)(ii).

ITEM	MINIMUM SPECIFICATIONS	STATEMENT OF COMPLIANCE
1.	**Brief Description of the Item being procured** The CMS team will primarily be composed of security analysts organized to detect, analyze, respond, report, and prevent cyber-security incidents. The main components of CMSP are the following: **Cyber Threat Intelligence Platform** – The platform is made up of threat intelligence feeds, alerts and reports that collect variety of threat information to different sources at the web, illegal trading sites, and Critical Information Infrastructure (CII) sector such as Energy, Financial, and Banking sector. **Network Protection Tools –** cyber security tools for CMSP's own network protection such as, but not limited to Firewalls, Antivirus, IPS/IDS, DDOS, Endpoint Detection and Response (EDR), and Network Advanced Threat Protection. **Monitoring Tools –** consist of tools that will monitor Cybersecurity Management System Project (CMSP) and priority agencies network to prevent data leak. **Log Collection and Correlation -** The system will aggregate the logs from the CMSP's chosen perimeter security tools and priority agencies. **Management Tools –** This component will be use as the initial step of incident response wherein severity of alerts and status of incidents will be shown via Graphical User Interface (GUI). Online ticketing and escalation of incidents to the SOC team can also be seen in the management tools.	

Artificial Intelligence (AI) / Machine Learning – The AI is responsible for the automated investigation of incidents. This includes rapid analysis, tracking, evidence collection, and forensics investigation that will help analysts to easily understand and respond to incidents.

Response System – this involves actionable intelligence that allows remediating current attacks which in return helps to prevent recursion of attacks. Escalation to Law Enforcement Agencies (LEAs) and reports also take place in the CMSP response system.

Portable SOC – a mobile device that can perform log scanning, analysis, detection, forensics investigation, and remediation to breaches and emergency incidents to government agencies, businesses and supply chains, and CIIs.

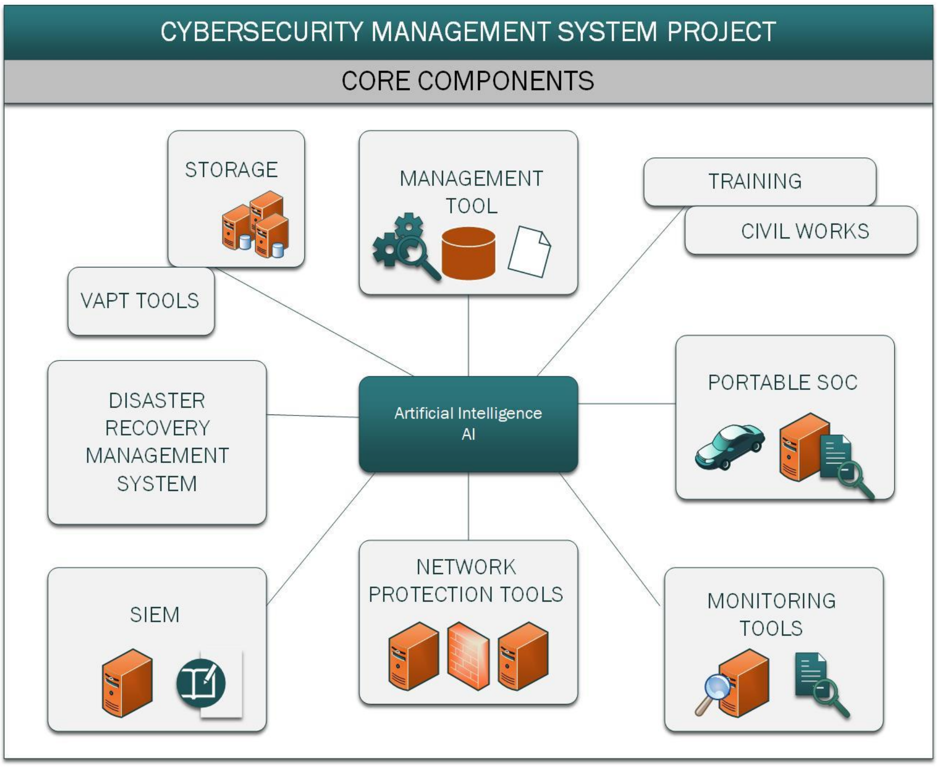
Disaster Recovery Management System – involves off-site disaster recovery, backup, and power management system that enable recovery or operation of the infrastructure in case of incident.

Other Physical Security Equipment – this involves the physical security systems in the CMSP such as Finger-Vein and keypad authentication, CCTV, and other SOC workstations.

Core Components	
Cybersecurity Management System	
Cyber Threat Intelligence Platform	
	Threat Intelligence Feeds
	Threat Data Alerts and Reports
	Web Intelligence
Network Protection Tools	
	Next Generation Firewall (NGFW)
	Distributed Denial of Service (DDoS) Protection
	Network Advance Threat Protection
	Endpoint Security
	IPS/IDS
	ADC
Monitoring Tools	
	Network Monitoring
	Vulnerability and Malicious File Detection
	Command and Control (C&C) Detection
	Lateral Movement Detection
Log Collection and Correlation	
Management Tools	
Artificial Intelligence	
	Automated Analysis
	Automated Investigation
	Threat Profiling
	DarkWeb Investigation
	Forensics

	i. Network Forensics ii. Endpoint Forensics	
	Response System i. Actionable Intelligence ii. Reports	
	Portable CMS	
	Disaster Recovery Management System	
	Offsite Disaster Recovery Management System	
	Backup Management System	
	Power Management System	
	Storage	
	VAPT Tools	
	Training and Services	
	Network Infrastructure	
	Other SOC Equipment and Civil Works	
2.	**Vendor Qualification**	
	2.1. General The Vendor shall be able to provide the following solutions: 2.1.1. Turn Key Solutions 2.1.1.1. Cyber Security Operations Center 2.1.1.1.1. Cyber Threat Intelligence Platform 2.1.1.1.2. Network Protection Tools 2.1.1.1.3. Monitoring Tools 2.1.1.1.4. Log Collection and Correlation 2.1.1.1.5. Management Tools 2.1.1.1.6. Artificial Intelligence 2.1.1.1.7. Portable SOC 2.1.1.1.8. Disaster Recovery Management System	
	2.1.2. SOC Set Up and provision of SOC workstations, Finger-Vein Biometric Authentication, switchable privacy glass, CCTV, network equipment, cables, furniture, and Video Wall Display including, but not limited to, systems that will assist the SOC and CERT to collect information, perform investigation and forensics of the collected data and respond to the breach in a proper and timely manner.	
	2.1.3. The Vendor shall be qualified to the following criteria: 2.1.3.1. The Vendor shall support the DICT with local service providers where applicable to optimize quality and timeliness of the service. 2.1.3.2. The Vendor shall develop and produce all the key offerings under this proposed solution. 2.1.3.3. The Vendor shall provide a valid certification from their previous client to prove their experience in providing similar solution in the government and/or private sector. For this project, "similar solution" shall mean "Security Operations Center (SOC) and/or same type of solution that will be deployed in the CMSP that has been offered in the previous client".	

	2.1.3.4. The Vendor shall provide a valid Business Registration Certificate (BRC) with a minimum of 5 years of experience in the field of intelligence, threat detection, and cyber security. 2.1.3.5. The Vendor shall provide a valid certification from at least two of their clients to prove that they performed cyber forensic investigations specifically involving external attackers. 2.1.3.6. The Vendor shall provide a portfolio or any documentary report to prove that they have deep intelligence in cyber threat actors especially those related to financial crimes and critical infrastructure. 2.1.3.7. The Vendor's methodology shall include forensic assessment of systems based on NBI (Network Based Indicators) as well as HBI (Host Based Indicators). 2.1.3.8. The Vendor must provide product specification and/or datasheet to prove that it has the technology to scale the forensic assessment to all Windows systems. 2.1.3.9. The Vendor shall be accessible 24x7 incident response hotline. 2.1.3.10. The Vendor shall provide product datasheet to prove expertise in the following: 2.1.3.10.1. Analysis of computer systems, network traffic transiting between customer's network and the Internet 2.1.3.10.2. Assessment of regular status report, assessment report of relevant findings, and recommendations for improvement and executive brief report 2.1.3.10.3. Executive-level briefing detailing necessary recommendations to improve incident preparedness capabilities 2.1.3.10.4. Computer security incident response support 2.1.3.10.5. Forensics, log and advanced malware analysis 2.1.3.10.6. Advanced threat actor response support 2.1.3.10.7. Advanced threat/incident remediation assistance	
3.	**Scope of Work** The scope of work shall be the following:	
	3.1. **SOC Setup** The Vendor shall set-up the whole Cybersecurity Management System Project (CMSP) of DICT. The design of CMSP shall be in accordance to the perimeter blueprints that DICT shall provide.	
	3.2. The Vendor shall provide the following: 3.2.1. SOC Workstations 3.2.2. Installation of SOC Physical Security Parameters such as CCTV, Keypad and Finger-Vein Biometric Authentication 3.2.3. Mantrap 3.2.4. Installation of Rack Cabinet 3.2.5. Installation of Video Wall 3.2.6. Installation of Switchable privacy glass	

	3.2.7. Installation of Fit Outs 3.2.8. Structured Cabling 3.2.9. Fire Suppression system for the CMS and server room 3.2.10. Civil Works as needed	
	3.3. The Vendor shall perform Vulnerability Assessment and Penetration Testing (VA/PT) for the SOC network.	
	3.4. The Vendor shall equip the SOC with cyber security tools for the SOC networks own protection such as but not limited to Firewalls, Anti-DDoS Protection, SOC Platform, Endpoint and Network Security, and Network Advanced Threat Protection.	
4.	**SOC Core Components**  CYBERSECURITY MANAGEMENT SYSTEM PROJECT CORE COMPONENTS STORAGE MANAGEMENT TOOL TRAINING CIVIL WORKS VAPT TOOLS DISASTER RECOVERY MANAGEMENT SYSTEM Artificial Intelligence AI PORTABLE SOC SIEM NETWORK PROTECTION TOOLS MONITORING TOOLS **Figure 4.1 SOC Core Components**	

5. **SOC Layout**

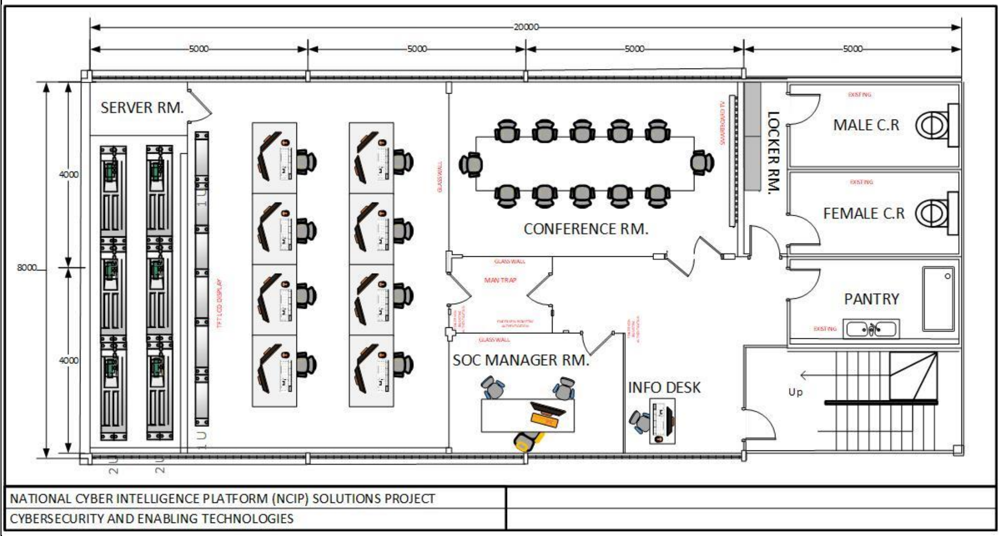


Figure 5.1 SOC Layout

Measurement: Centimeter (cm)

6. **Deployment**

6.1. For the 1st year, the solution shall cover ten (10) organizations in up to ten (10) different physical sites. These organizations are DICT, NSC, DND, DFA, PCOO, OP/PMS, DOE, DBM, DOF and NICA.

6.2. The solution shall cater three (3) years growth and shall support a minimum additional twenty (20) agencies each year.

1st Phase	2nd Phase	3rd Phase
2018	2019	2020
10 Agencies	**20 Agencies**	**20 Agencies**

6.3. The solution shall be deployed in a geo-distributed fashion, monitoring and protecting multiple sites and locations.

6.4. The solution shall allow for geo-distributed monitoring, detection and forensics capture, while centralizing the processing of alerts into incidents and the investigation of those incidents.

6.5. The solution shall allow for robust and scalable geo-distributed deployment without requiring extensive network bandwidth allocated. The solution shall support a scenario where traffic is forwarded to a central location for processing.

6.6. The solution shall allow for distributed initial processing of raw data and communication of metadata and lightweight commands only over the internet.

6.7. The solution shall allow for distributed deployment, where the different subsystems can communicate over WAN (in case dedicated private lines of fiber are not available).

	6.8. The solution shall allow and facilitate secured, encrypted communication channels between its subsystems in general and remote, distributed ones in particular. 6.9. The investigation systems and interfaces must be centralized for ease of deployment, completeness and integrity of the investigation. 6.10. The solution shall be able to query the remote distributed sites as part of the automated/manual investigation, seamlessly and transparently for users across the different sites, in a unified manner. 6.11. Management and updates of the solution shall be centrally managed. 6.12. The solution shall be able to be deployed in a multi-agency mode where one system protects multiple organizations, providing economy of scale while respecting data and access separation requirements between organizations. 6.13. The solution shall allow an organization to protect multiple sub-organizations, divisions, business units and subsidiaries with one, unified yet extensible deployment. 6.14. The solution shall allow for monitoring of different organizations which can be centralized (traffic forwarded to central location for full processing), distributed (initial processing in remote sites, central follow up investigation), or hybrid between protected organizations. 6.15. Data separation (alerts, incidents, evidences, configurations) between organizations is maintained under one multi-organization deployment. 6.16. Learning, rules, intelligence, enrichments, and predefined rules can be leveraged across organizations. 6.17. User roles and permissions model must allow for access and handling separation between organizations and between analysts to meet customers' needs and to respect their confidentiality. 6.18. The solution shall natively support a single-agency and multi-agency deployment scenarios. 6.19. The solution software (SW) components should be agnostic to hardware (HW) components and vice versa. 6.20. The solution shall generate health status of physical hardware and security tools inside the SOC. 6.21. The solution must be configured to Simple Network Management Protocol (SNMP) for consistent visibility and monitoring of all systems. 6.22. Vendor should include all necessary hardware, system storage, database, and backup for the software or system in order to ensure continuity of operations. 6.23. The Solution must be hybrid based solution and ensure availability for 99.9% of the time during each calendar month 6.24. The solution shall support all operations of the CMSP.	
7.	**CMSP Core Components**	
	7.1. Technical Specifications 7.1.1. Functionality / User Requirements Threat Intelligence Feeds shall come from the energy and financial sector especially from banking & finance aside from darknet and illegal trading sites.	

	7.1.1.1. **Cyber Threat Intelligence Platform** – The Sources shall come from the Critical Information Infrastructures (CIIs) Sector, International and Local, such as, but not limited to Energy and Finance especially from the Banking and Supply Chains, including Web Intelligence from the Darknet and Illegal Trading sites. The sources shall support Hybrid Technology with external sources coming from the Cloud and an On-Premise Technology that will support the internal threats. The solution shall also provide intelligence about the current threat landscape of the Philippines.	
	7.1.1.1.1. **Threat Intelligence Feeds** 7.1.1.1.1.1. The solution shall support online daily intelligence updates and threat data in the CMS such as but not limited to: 7.1.1.1.1.1.1. APT Reports 7.1.1.1.1.1.2. Ransomware Incidents 7.1.1.1.1.1.3. Malicious Hashes 7.1.1.1.1.1.4. Botnet C&C URL Feeds 7.1.1.1.1.1.5. Cyber Espionage 7.1.1.1.1.1.6. Hardware and Software Vulnerabilities 7.1.1.1.1.1.7. IP Reputation Feeds	
	7.1.1.1.1.2. The solution shall provide detailed description of malware family. 7.1.1.1.1.3. The solution shall provide intelligence to known APT Groups. 7.1.1.1.1.4. The system shall include real-time vulnerability intelligence feed and patch management workflows based on active and evolving exploits and vulnerabilities that is critical in each organization. Remediation to each vulnerability shall be included in the system. 7.1.1.1.1.5. The solution shall include mobile malicious hashes, Command and Control (C&C), and botnets feed. 7.1.1.1.1.6. The system shall be able to share and transmit recent threat data to all priority agencies and detection sensors with full recommendation and remediation in the threats. 7.1.1.1.1.7. The solution shall include threat data feeds that match the data sources for detection, and able to create custom rules.	
	7.1.1.1.2. **Threat Data Alerts and Reports** 7.1.1.1.2.1. The solution shall provide real time alerts and constantly updating streams of threat data with remediation and recommendation to Human Analyst. 7.1.1.1.2.2. The solution shall include threat data reports and alerts to illegal cyber activities such as but not limited to: 7.1.1.1.2.2.1. Cyber crime 7.1.1.1.2.2.2. Hacktivism 7.1.1.1.2.2.3. Illegal Trading Sites	

	7.1.1.1.2.2.4. Financial Threats 7.1.1.1.2.3. The solution shall collect threat data from different web sources including social media platforms, deep-web sites, darknet platforms, and more. 7.1.1.1.2.4. The solution shall be able to generate actionable intelligence and recommendations base on the reported illegal cyber activities. 7.1.1.1.2.5. The solution shall support multiple languages that may help in understanding and securing the country from cyber threats in different web sources.	
	7.1.1.1.3. **Web Intelligence** 7.1.1.1.3.1. The solution shall be able capable of collecting information from open source, deep websites, and dark websites. 7.1.1.1.3.2. The solution shall support collection of important information from different social media platforms such as Facebook, Twitter, YouTube, Instagram, Onion Sites, LinkedIn, Viber, Telegram, and other Media Sites. 7.1.1.1.3.3. The solution shall provide a framework that will help human analyst in harvesting information of the specified target from any web site such as Social Networks, Dark websites, Blogs, etc. 7.1.1.1.3.4. The solution shall engage in different social media platforms and sites. 7.1.1.1.3.5. The solution shall be able to collect information from different social media account of the specified target in a single click manner. 7.1.1.1.3.6. The solution shall support programing language like JAVA, C#, PHP, JavaScript, etc., during the scenario execution in order to provide a way to call external services like translation or social network API request. 7.1.1.1.3.7. The solution shall access web sites while hiding the user's IP address and other identifiable information. The solution will be able to access websites using TOR access. 7.1.1.1.3.8. The solution shall support crawling "darkweb sites" (i.e.: domain, onion) which are hidden and inaccessible sites to regular Web browser (non-search engine indexed sites). In addition, it shall provide a configuration to any social network or site, covertly, and check the changes of the updates on frequent intervals; such sites are mostly not indexed in Google. 7.1.1.1.3.9. The solution shall have a GUI for management and monitoring which provides the ability to optimize bandwidth usage, by monitoring the efficiency of resource utilization, including bandwidth, engines,	

	crawler units, and sites. In addition, it shall provide ongoing operational monitoring and alerts on any malfunction or problem. 7.1.1.1.3.10. The solution shall provide its users the means to schedule collection tasks. The solution shall support managing tasks, distribute them between different crawlers and coordinate them in order to generate full scenario. 7.1.1.1.3.11. The collection solution shall be able to support multiple running tasks. Each is based on a different flow of work. In addition, the solution will provide monitoring tools to track process and status of all running tasks. 7.1.1.1.3.12. The solution shall be scalable and allow scale up by adding additional crawlers to the system. 7.1.1.1.3.13. The user shall be able to perform all management operation including crawling configuration through a web based UI interface. 7.1.1.1.3.14. The solution shall provide a convenient approach for social download, meaning downloading the related web accounts to the target web account profile. 7.1.1.1.3.15. The solution shall collect data from any site that support displaying html content. The collection platform shall provide a way to access restricted section inside sites such as login to a social network or a forum. All data presented in the page can be harvested like user comments and reply to a comment, attachments, etc.	
	7.1.1.1.3.16. The solution shall support the following effective approaches: 7.1.1.1.3.16.1. Structured Crawling - Scenario based collection (a.k.a robots definition) 7.1.1.1.3.16.2. Web API based data extraction (e.g. Facebook API) 7.1.1.1.3.16.3. RSS extraction (RSS content and link content) 7.1.1.1.3.16.4. Unstructured crawling (a generic mechanism to extract data that is not based on predefined scenario) 7.1.1.1.3.17. The solution shall support running java scripts (browser based crawling) in order to crawl data from site that support AJAX technology. 7.1.1.1.3.18. The solution shall overcome challenge-response test used by websites (CAPTCHA) and shall support a set of rich full variations of CAPTCHA that might occur in the crawling process at any stage. 7.1.1.1.3.19. The solution shall support a browser add-on that will enable the analyst to issue crawling requests while	

browsing the web. The solution shall provide ways to customize and randomize the human actions.

7.1.1.1.3.20. The solution shall provide Graphical UI to the human analyst showing the link and comparison of social accounts of the specified target for better understanding of its behavior.

7.1.1.1.3.21. The solution shall provide a user interface to extract the value from selected section of the webpage, extract attributes from html tags, download resource (i.e. picture, avatar), and extract URL and page URL.

7.1.1.1.3.22. The solution shall provide a user interface to build any http web flow requiring action such as load URL, click, scroll to bottom, press enter, input text, repeated click, select button, select radio, set checkbox, create loop for repetition.

7.1.1.1.3.23. The solution shall provide method to overcome http error anti-bot website by retrying or/and using different collection method.

7.1.1.1.3.24. The solution shall provide ways to overcome http timeout, extraction time-out.

7.1.1.1.3.25. The solution shall mimic human actions in order to avoid being detected as a robot.

7.1.1.1.3.26. The solution shall provide mimic human profile to define the randomized action. The profile can be set for a selected website or/and reuse several website with a 2 clicks configuration.

7.1.1.1.3.27. The solution shall be able to manage bank of web accounts that will be used as agents in order to access restricted section in sites such as Social Networks, Forums, etc. The solution shall support a capability to schedule the harvest task in a way that the same account will not be used simultaneously and allocate specific task to a specific agent (social engineering).

7.1.1.1.3.28. The solution shall be able to support multiple running tasks. Each is based on a different flow of work. In addition, the solution will provide monitoring tools to track process and status of all running tasks.

7.1.1.1.3.29. The solution shall normalize all crawled data shall into general, structured storage, facilitating future searches and analysis. Collected Data will be further processed in order to eliminate duplications and ensure updated/new data only (deleted will be kept).

	7.1.1.1.3.30. The solution shall provide convenient and visual approach for configuring crawling functionality, either by Professional services or a person assigned by the organization. 7.1.1.1.3.31. The solution shall be capable of interfacing with 3rd party analytics systems to provide access to collected data. 7.1.1.1.3.32. The solution shall be scalable and allow scale up by adding additional crawlers to the system. 7.1.1.1.3.33. The solution shall provide a convenient approach for social download, meaning downloading the related web accounts to the target web account profile. 7.1.1.1.3.34. The solution shall support geolocation accordingly from geo-supported web sites.	
	Web Engagement 7.1.1.1.3.35. The solution shall include Avatars, and the means of using these Avatars in Open source platforms as well as the Dark Web. 7.1.1.1.3.36. The solution shall enable avatar configuration, including a minimum of login, password, proxy, description settings. 7.1.1.1.3.37. The solution shall allow the system analysts / administrators to generate new Avatars. 7.1.1.1.3.38. The solution shall enable Avatars utilization by the collection platform to collect information via avatar in an automatic manner or by defining the specific Avatar for the collection job. 7.1.1.1.3.39. The solution shall include a secured browser as a complementary tool that enables the analyst to conduct online operations using crafted avatars. 7.1.1.1.3.40. The solution’s secured browser shall ensure that online browsing is secured and anonymous. 7.1.1.1.3.41. The solution’s secured browser shall be able to access the web using the avatar originating country IP address. 7.1.1.1.3.42. The solution’s secured browser shall be able to prevent certain human error mistakes by locking the keyword to specific languages (according to the avatar cover story), notifying the analyst before committing an intrusive action, and more. 7.1.1.1.3.43. The solution’s secured browser shall be able to emulate a browser configuration, thus meeting the cover story of the avatar (such as automatic login). 7.1.1.1.3.44. The solution’s secured browser shall be able to verify that the single virtual entity will not be used simultaneously by 2 analysts.	

		7.1.1.1.3.45. The solution’s secured browser shall be able to audit the avatar’s activities. 7.1.1.1.3.46. The analyst shall be able to use secured browser to do conduct manual social engineering activities (e.g. post, comments, like). 7.1.1.1.3.47. The solution’s secured browser shall automatically analyze the web page and get meaningful information without leaving the page. Such information includes entity extraction in English and various languages, such as Tagalog / Filipino. 7.1.1.1.3.48. The solution shall include a minimum of 50 mature avatars.	
		Analytics 7.1.1.1.3.49. The solution shall enable users to perform investigations based on topics, targets, and groups of targets. 7.1.1.1.3.50. The solution shall provide ready to use tools and screens to view the collected data. Each type of data should be presented in a way that fits it (e.g. information about a person in a social media network should include personal details, list of friends, list of historical social activities, list of related groups, list of photos and videos, etc.). 7.1.1.1.3.51. The solution shall include a built in general search mechanism that gives the tools to quickly search data of all types (documents, web pages, social accounts, groups, etc.) by various dimension. 7.1.1.1.3.52. The solution shall allow a clientless installation of the analytics platform so that the user will be able to work from any workstation using an applicable web browser. 7.1.1.1.3.53. The solution shall include a built in ability to identify well known text structures such as names of people, locations, phone numbers, credit card numbers, URLs, email addresses, etc. The solution shall be able to mark and color the identified entities within the text. The solution shall also provide statistical view of the identified entities by type. For example, the top mentioned URLs per case or per person. 7.1.1.1.3.54. The solution shall be able to investigate persons of interest that are actually a unification of several internet identities. The solution shall recommend the analyst that few identities of different social networks are suspected to be of the same person.	

	7.1.1.1.3.55. The solution shall correlate profiles and provide relationship analysis between two entities to display common activities, friends, etc. 7.1.1.1.3.56. The solution shall enable image analysis using collected images. Image analysis capabilities shall include the following: 7.1.1.1.3.56.1. Label Detection - Detect categories within an image, such as weapons, vehicles, places, etc. 7.1.1.1.3.56.2. Face Detection - Detect multiple faces within an image, along with the associated key facial attributes like emotional state or wearing headwear. 7.1.1.1.3.56.3. Logo Detection - Detect popular product logos within an image. 7.1.1.1.3.56.4. Landmark Detection - Detect popular natural and man-made structures within an image. 7.1.1.1.3.57. The solution shall provide relationship analysis between two profiles to display common activities, friends, etc. 7.1.1.1.3.58. The solution shall automatically reveal data from private profiles (protected by privacy settings) from scattered public information, and provide the investigators with enlightening data about those virtually invisible entities. 7.1.1.1.3.59. The solution shall include a built in Report engine in order to display all retrieved data for a specific account in PDF and WORD format.	
	Online Awareness 7.1.1.1.3.60. The solution shall enable collection and access in near real-time data from popular social media websites, including, but not limited to: 7.1.1.1.3.60.1. Facebook 7.1.1.1.3.60.2. Twitter 7.1.1.1.3.60.3. YouTube 7.1.1.1.3.60.4. LinkedIn 7.1.1.1.3.60.5. Popular news websites from around the world 7.1.1.1.3.60.6. Popular blogs from around the world 7.1.1.1.3.60.7. Instagram 7.1.1.1.3.60.8. YikYak 7.1.1.1.3.60.9. Vbulletin 7.1.1.1.3.61. The solution shall enable access to near-real time activity of interest from the services supported under Situational Awareness.	

	7.1.1.1.3.62. The solution shall harvest the data sources supported under Situational Awareness for primary search operators, and in addition filter the data as defined by the user.	
	7.1.1.1.3.63. The solution shall enable the user to use primary, secondary, and tertiary search operators (i.e. either individual words, key phrases, or co-located and disparately located words) contained within social media accounts, websites of interest, and location data. The user shall be able to define cross-referencing of one or more of these search operators.	
	7.1.1.1.3.64. The solution shall enable the user to create groups of search terms so that they can be organized by subject area. The user shall be able to add single words, multiple words and phrases as search criteria.	
	7.1.1.1.3.65. The solution shall enable the user to view and filter all the results on a map view.	
	7.1.1.1.3.66. The solution shall enable the user to search for emoticons within the result set via alphabet letters.	
	7.1.1.1.3.67. The solution shall enable the user to block certain social network entities from all results set and collections.	
	7.1.1.1.3.68. The solution shall not be limited by any physical or environmental boundaries with respect to monitoring of social media content. Its reach shall be global.	
	7.1.1.1.3.69. The solution shall enable the user to configure the period for which data is collected and stored.	
	7.1.1.1.3.70. The solution shall enable the user to search for results based on location. The user shall be able to search based on geographical location (i.e. by Longitude and Latitude or by location name).	
	7.1.1.1.3.71. The solution shall enable the user access to the street view of the actual location (where available via Google Street View).	
	7.1.1.1.3.72. The solution shall enable the user to setup a query for all data sources at once based on location and keywords. The solution shall be able to collect constant data from all sources in near real time based on the query.	
	7.1.1.1.3.73. The solution shall enable the user to duplicate / clone all location based queries, and create new ones based on the same parameters.	

	7.1.1.1.3.74. The solution shall enable the user to stop location based queries and keep all the data available for viewing. 7.1.1.1.3.75. The solution shall have a responsive and rich GUI which enables the user to use the tool efficiently. 7.1.1.1.3.76. The solution shall include a user dashboard that provides access to creating profiles, mapping, storing extracted data in a vault, and reporting functionality. 7.1.1.1.3.77. The solution shall enable the user to depict a high-level view of all the activities carried out in the saved profiles. 7.1.1.1.3.78. The solution shall support various user types. Administration privileges shall be available for users in management and admin positions. 7.1.1.1.3.79. The solution shall support identification of key open-source influencers by ranking profiles based on user predefined search operators (e.g. profile usability and popularity). 7.1.1.1.3.80. The solution shall enable users to visualize Twitter posts / conversations between accounts. 7.1.1.1.3.81. The solution shall enable users to view activity and geo-location of specific suspicious profiles / accounts (i.e. without geo-location or keyword search) to enable a comprehensive view of that profile's activity. 7.1.1.1.3.82. The solution shall be able to analyze all the content from the search results and present it as a word cloud. 7.1.1.1.3.83. The solution shall have a rich alerts mechanism for creating alerts on active real time queries and tracking certain target activities. This alert mechanism shall enable the user to setup email or mobile phone SMS based alerts on all the above. 7.1.1.1.3.84. The solution shall support search of historical events. The user shall be able to issue a historical query on a location and receive social media results from that location for the desired time period. 7.1.1.1.3.85. The solution shall enable the user to search for accounts using one of the following parameters: email account, Facebook username, and Twitter username. 7.1.1.1.3.86. The solution shall simplify the presentation of complex data to enable timely and accurate operational decision making.	

		7.1.1.1.3.87. The solution shall be able to produce summary reports of ‘posts of interest’ based on cross-referenced searches as defined by the user. 7.1.1.1.3.88. The solution shall be able to produce summary reports of ‘posts of interest’ based on the geographic location of the post, either based on GPS coordinates of the post, or by inferring the location (i.e. a location’s name in the body of the post or the biography of the user). 7.1.1.1.3.89. The solution shall generate reports that summarize key information in a user friendly dashboard. 7.1.1.1.3.90. The solution shall enable the user to bookmark and store certain posts for later access. The solution shall support generation and export of a single CSV that includes such bookmarked results.	
		Social Media Profiling 7.1.1.1.3.91. The solution should have a responsive and rich GUI which enables the user to use the tool efficiently. 7.1.1.1.3.92. The solution’s GUI shall be similar to a search engine based to vendor identify database. 7.1.1.1.3.93. The solution shall enable searching based on criteria, such as, but not limited to: phone, name, nickname, email, etc. 7.1.1.1.3.94. The solution shall provide results on personal information, such as, but not limited to: name, phone, email, address, nickname, friends, etc. 7.1.1.1.3.95. The solution shall provide in its results the social media related accounts (Facebook, twitter, Instagram, etc.) 7.1.1.1.3.96. The solution shall be able to trigger collection of social media account information of the target in a single click. 7.1.1.1.3.97. The solution shall provide web pages related to the mentioned target. 7.1.1.1.3.98. The solution shall provide mobile applications related to the target, including information such as, but not limited to: avatars, name, last time seen (when relevant) for apps like WhatsApp, Line, skype, WeChat, etc. 7.1.1.1.3.99. The solution shall be able to create insights and comments. 7.1.1.1.3.100. The solution shall be able to provide reports of the target identity discovery.	
		Security 7.1.1.1.3.101. The solution shall provide a security layer between the Web Collection platform and the Web Analytics	

	platform, which contains knowledge and investigation conclusions to inspect suspicious data. 7.1.1.1.3.102. The solution shall provide an automated data cleaning and cleansing layer between the Web Collection platform and the Web Analytic platform	
	7.1.1.2. Network Protection Tools 7.1.1.2.1. **Next Generation Firewall** (200 Gbps Firewall throughput) 7.1.1.2.1.1. Services and Functionality 7.1.1.2.1.1.1. The solution shall have a link and path failure detection capability in addition to device failure. 7.1.1.2.1.1.2. The solution shall support authentication for both client and session. 7.1.1.2.1.1.3. The solution shall be able to support IPv6 traffic in terms of 6 to 4 Network Address Translation (NAT) or 6 to 4 tunneling at the same time able to track, log and view different displays of IPv6 routing tables for various customers' security context in CLI and GUI 7.1.1.2.1.1.4. The solution shall support traffic encrypted with SSL, the NGFW must be able to selectively apply a policy-based decryption and then inspect the traffic for threats, regardless of ports. 7.1.1.2.1.1.5. The solution shall have a correlation engine that looks for predefined indicators of compromise network-wide, correlates matched indicators, and automatically highlights compromised hosts, reducing the need for manual data mining. 7.1.1.2.1.1.6. The solution shall have local database of URL categories for faster response. 7.1.1.2.1.1.7. The solution shall be able to identify unknown malware by using multi-method detection technology, such as static, dynamic, and bare metal analysis. 7.1.1.2.1.1.8. The solution shall be able to provide context around attacks, such as who is the attacker, the campaigns it is involved, and including which industries are being targeted. 7.1.1.2.1.1.9. The solution shall have "indicators of compromise" (IOCs) tagging for alerting organization when a specific threat has been observed in the organization or similar industry.	

7.1.1.2.1.1.10. The solution shall be capable of creating threat protections by directly exporting IOCs lists that can be automatically enforced as policy, and also imported to the third-party.

7.1.1.2.1.1.11. The solution shall have integrated IPS, anti-spyware, anti-malware, and Command-and-Control (C2) prevention capabilities.

7.1.1.2.1.1.12. The solution shall have visibility on the applications, users, and contents such as data filtering (ex. Block specific Personal Identifiable Information or PII inside a document) and file blocking (ex. Block specific file types).

7.1.1.2.1.1.13. The solution shall be able to deploy consistent policies to local and remote users running on different Operating System (OS) such as but not limited to Windows, MAC, and Linux.

7.1.1.2.1.1.14. Enforcement of security rules for the access control shall have at least 150 predefined/services/protocols at time intervals with an expiry date and time must be configurable.

7.1.1.2.1.1.15. The solution shall be able to support integration with Active Directory, TACACS, RADIUS, digital certificates and tokens (ie SecureID) on the gateway and configurable local user database for user authentication and authorization without the need for an external device

7.1.1.2.1.1.16. Security management application must only be managed by administrator accounts and can co-exist with security gateway. Additional log servers must be supported by gateway but central logging and searches must be done on the security management appliance. Otherwise, a browser-based access is a must. For easy viewing and basic settings configuration, a front LCD panel display is a must.

7.1.1.2.1.1.17. Application control and URL Filtering security rules must be unified for easy configuration and is able to categorized more than 200 million URLs sites which can support multiple categories by creating a filtering rule and creation of filtering for single site by multiple categories. These rules must be configurable

	with limiting application usage based on bandwidth consumption, blacklisting and whitelisting of URL regardless of the category and blocking notification modification options and redirection of the user to a remediation page. 7.1.1.2.1.1.18. The solution shall support real-time manner to inform or ask users to educate or confirm their actions based on the security policy and an easy-to-use searchable interface for applications and URLs must be supported 7.1.1.2.1.1.19. The solution shall limit the unauthorized transfer of files and sensitive data, and safely enables non-work-related web surfing. 7.1.1.2.1.1.20. The solution shall identify unknown malwares and analyse it based on hundreds of malicious behaviors, and then automatically create and delivers protection. 7.1.1.2.1.1.21. Anti-Bot and Anti-Virus application using multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications to detect and stop suspicious abnormal network behavior must be integrated on the next generation firewall.	
	7.1.1.2.2. **Distributed Denial of Service (DDoS) Protection** 7.1.1.2.2.1. **Technical Services** 7.1.1.2.2.1.1. The solution shall be able to protect CMSP's internal network from DDoS attack in a hybrid deployment. 7.1.1.2.2.1.2. The solution shall have a proactive incident response to contain and block potential DDoS attacks without affecting normal network traffic. 7.1.1.2.2.1.3. The solution shall have an access portal that will provide transparent attack mitigation visibility and reporting before, during, and after an attack. 7.1.1.2.2.1.4. The solution shall have a scrubbing center located in the cloud to provide the volumetric DDoS protection. 7.1.1.2.2.1.5. The solution shall have DDoS protection service against low and slow attack. 7.1.1.2.2.1.6. The solution shall have on premise protection against volumetric, state-exhaustion and application-layer DDoS attacks. 7.1.1.2.2.1.7. The solution shall not have costs associated with size of DDOS Attack and should provide protection from unlimited number of DDoS attack incidents.	

7.1.1.2.2.1.8. The solution shall not have costs associated with reporting or administrative changes.

7.1.1.2.2.1.9. The solution shall stop DDoS attacks hidden in encrypted traffic whether IPv4 or IPv6.

7.1.1.2.2.1.10. The solution shall have real-time updates on DDoS protection from active botnets, advanced web crawler, GeoIP Tracking and Domain and IP reputation through Intelligence Feed with actionable intelligence

7.1.1.2.2.1.11. The solution shall be able to detect and prevent the following:

7.1.1.2.2.1.11.1. Invalid Packets

7.1.1.2.2.1.11.2. Spoofed TCP SYN Flood

7.1.1.2.2.1.11.3. Malformed DNS requests

7.1.1.2.2.1.11.4. Excessive amounts of traffic according to configurable thresholds

7.1.1.2.2.1.11.5. Specified TCP/UDP ports with payloads matching or not matching a configurable regular expression

7.1.1.2.2.1.11.6. Traffic from any host that generates more consecutive failed DNS requests than the configured limit

7.1.1.2.2.1.11.7. Idle TCP sessions and blacklist consecutive fails

7.1.1.2.2.1.11.8. Malformed HTTP packets

7.1.1.2.2.1.11.9. Specific HTTP packets with HTTP headers matching configurable REGEX expressions

7.1.1.2.2.1.11.10. Hosts exceeding a configurable threshold for total number of HTTP operations per second, per destination server

7.1.1.2.2.1.11.11. TCP SYN floods

7.1.1.2.2.1.11.12. ICMP floods

7.1.1.2.2.1.11.13. Sources that repeatedly interrupt HTTP requests

7.1.1.2.2.1.12. Protection services configuration must have pre-defined settings on these services: Web, DNS, VoIP, Mail, Rlogin, File, or a Generic Server and parameters can be changed while it is running like adding black list based on host IP, country, domain and URL and controls of individuals or all protection services.

7.1.1.2.2.2. **General Requirements for DDoS Mitigation**

7.1.1.2.2.2.1. The vendor shall describe their pedigree in DDoS mitigation and demonstrate an effective track record.

7.1.1.2.2.2.2. The solution shall support both DNS redirect (per IP) and Border Gateway Protocol (BGP) redirect (per

	Class C). Both options must be available within the same network, same web portal and managed by same support team. 7.1.1.2.2.2.3. The solution shall leverage IP Anycast. 7.1.1.2.2.2.4. The solution shall be fully owned, operated and managed by the successful vendor. Support shall be provided directly by the vendor for DDoS events. 7.1.1.2.2.2.5. The solution shall be PCI-DSS compliant. Please provide date of last certification. 7.1.1.2.2.2.6. The solution shall intelligently integrate with on premises hardware (hybrid).	
	7.1.1.2.2.3. **Platform Architecture** 7.1.1.2.2.3.1. The vendor shall describe their network and scrubbing center architecture in with as much transparency as possible. 7.1.1.2.2.3.2. The solution shall provide at least 1.5Tbps of dedicated attack capacity. 7.1.1.2.2.3.3. The solution shall have dedicated attack transit. 7.1.1.2.2.3.4. The solution shall provide a list of their geographic scrubbing locations. The network layer scrubbing capacity at each location must be provided. 7.1.1.2.2.3.5. The solution shall be mitigated to common network layer DDoS attacks as well as complex multisector attacks. Please describe how the platform adapts to changing vectors. 7.1.1.2.2.3.6. The solution shall allow customer to add and edit mitigation rules specific to each IP address and Class C address range. These firewall rules should allow blacklisting and whitelisting of certain IP's, ports and protocols. 7.1.1.2.2.3.7. The solution shall allow customer to connect multiple GRE tunnels to any scrubbing location. 7.1.1.2.2.3.8. The solution shall provide 500Mbps or clean traffic via GRE, with ability to burst up to 5Gbps. 7.1.1.2.2.3.9. The solution shall allow Border Gateway Protocol (BGP) peering between customer site and the platform. 7.1.1.2.2.3.10. The vendor shall describe in detail the process to route on/off the platform. This must not involve on the fly BGP configuration updates the CMS. 7.1.1.2.2.3.11. The vendor shall describe the options to automate this route on/off process. 7.1.1.2.2.3.12. The solution shall allow per application redirections (DNS Redirect) to inspect and block application layer DDoS.	

	7.1.1.2.2.3.13. The solution shall allow traffic such as API's and on ports other than 80/443 to be proxied. 7.1.1.2.2.3.14. The solution shall provide the ability maintain the source IP address in the case where SSL cannot be loaded into the platform. Explain how this is achieved. It is understood these limits mitigations to application layer. 7.1.1.2.2.3.15. The solution shall provide a dedicated IP address per application for DNS redirect.	
	7.1.1.2.2.4. **Detection and Alerting** 7.1.1.2.2.4.1. The solution shall support monitoring of SOC's edge routers. The alerts should be triaged by vendor SOC Analysts to prevent excessive alerting. 7.1.1.2.2.4.2. The solution shall be able to integrate on premises network firewall. 7.1.1.2.2.4.3. The solution shall be able to integrate on premises web application firewall. 7.1.1.2.2.4.4. The solution shall signal bad actor IP data to the platform for blocking in real time. 7.1.1.2.2.4.5. The solution shall provide integration with SOC's SIEM. 7.1.1.2.2.4.6. The solution shall provide email/phone and SMS alerting options.	
	7.1.1.2.2.5. **Web Portal** 7.1.1.2.2.5.1. The solution shall provide detailed insight into attacks and configuration via web portal. 7.1.1.2.2.5.2. The solution shall provide the ability to customise dashboards via the web portal. 7.1.1.2.2.5.3. The solution shall allow ease of proxy and BGP/GRE configuration set up and changes via web portal. 7.1.1.2.2.5.4. The solution shall allow unlimited users access via web portal. Customer shall be able to create additional users as required. 7.1.1.2.2.5.5. The solution shall provide multi-tenant access via web portal in the event businesses within the group need a sub account. 7.1.1.2.2.5.6. The solution shall provide the option of two factor authentication.	
	7.1.1.2.2.6. **SOC Support** 7.1.1.2.2.6.1. The solution shall be supported by a 24/7 Security Operation Center operated by the vendor. 7.1.1.2.2.6.2. The SOC Analysts shall be Tier II Analysts able to provide insight and expertise and not a simple help desk. 7.1.1.2.2.6.3. The SOC Analysts shall be available 24/7 via phone, email and chat support.	

	7.1.1.2.2.6.4. The SOC Analysts shall be fully equipped to handle the majority of configuration and attack related requests. 7.1.1.2.2.6.5. The solution shall be supported by extensive documentation to help the user in configuring and using the DDoS mitigation service.	
	7.1.1.2.3. **Network Advance Threat Protection** 7.1.1.2.3.1. The solution shall include network threat protection sensor that support Inline blocking mode or span/tap mode. 7.1.1.2.3.2. Update of VM used for Dynamic Analysis can be done from the GUI without an OS upgrade. VM is built, maintained, and delivered by the vendor. 7.1.1.2.3.3. Detection appliances shall be capable of automatically downloading threat intel from an intelligence cloud. 7.1.1.2.3.4. Detection appliance OS software shall automatically be updated from the Web management GUI. 7.1.1.2.3.5. Detection appliances shall support inline monitoring and blocking. VM images for malware detonation shall be upgradable from the Web Management GUI. 7.1.1.2.3.6. The solution shall be able to run multiple Micro Tasks in a single VM (e.g. run sample across multiple versions of Adobe Acrobat in a Single VM Execution). 7.1.1.2.3.7. The solution shall allow the export of reports and alerts relating to malware in PDF format. 7.1.1.2.3.8. The solution shall be able to send automated health alerts through SMTP to preconfigured destinations. 7.1.1.2.3.9. The solution shall allow the creation of accounts with different roles used to administer the solution, or just monitor the alerts. 7.1.1.2.3.10. The solution shall be administered through a web-based console that doesn't require the installation of additional software. 7.1.1.2.3.11. The solution shall be able to send event notifications using format standards such as JSON and XML. 7.1.1.2.3.12. The solution shall be able to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, SNMP, or HTTP POST) and standard formats (e.g. JSON and XML). 7.1.1.2.3.13. The solution shall have a health check portal on the GUI displaying system software, system hardware and file system information. 7.1.1.2.3.14. The solution shall have its logs archived locally, and they should be downloadable via the GUI. 7.1.1.2.3.15. The solution shall be able to generate real-time Malware Notification Alerts via The System Console, Simple Network	

	Management Protocol, Web Alerts via HTTP and/or HTTPS, and Email. 7.1.1.2.3.16. The solution shall be able to utilize NetBIOS and DNS for hostname resolution when generating alerts. 7.1.1.2.3.17. For the above list of applications supported in the VM's the Vendor must have a method for pushing updates to the list of applications dynamical to the appliance without requiring a full OS or solution upgrade. 7.1.1.2.3.18. The solution shall utilize hardened Virtual Machine (on-premise) technology to positively identify malware, including zero-hour vulnerability exploits, polymorphic payloads, and obfuscated java-script. The virtualization solution shall not be detectable by malware in order to avoid evasion. The Hypervisor must not be an OEM solution such as from VMWare. 7.1.1.2.3.19. The analysis must be performed runtime in order to detect all the malware actions, even the ones that fail in the virtual environment but might be successful on a client workstation. Before and After differential comparison or VM state is not acceptable. 7.1.1.2.3.20. The solution shall be able to detect and report web exploits by using multiple versions of web browsers and plug-ins. 7.1.1.2.3.21. The solution shall be able to detect and report malware downloaded by users or downloaded in the context of a web exploit by using multiple client operating systems with multiple service pack levels. 7.1.1.2.3.22. The solution shall be able to automatically generate a network communication profile if the malware tries to contact network resources during the analysis. This profile shall be used to determine if systems on the network are compromised. 7.1.1.2.3.23. The solution shall be able to simulate end used actions in order to force the execution of malware that rely on triggers from and end user, like a mouse click. 7.1.1.2.3.24. The solution should be able to detect and prevent advanced Malware, Zero-day attack and targeted Advanced Persistent Threat without relying on just Signature database. 7.1.1.2.3.25. solution shall perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero-day and targeted attacks. No information should be send to third party systems or cloud infrastructure system for analysis and detection of Malware. 7.1.1.2.3.26. The solution shall have the ability to detect multi-stage attacks and must not be a file-based Sandbox technology which is limited to examining one file at a time in isolation.	

		7.1.1.2.3.27. The solution shall automatically detect and confirm multistage zero-day malware and targeted attacks without prior knowledge of the malware. 7.1.1.2.3.28. Solution should utilize a stateful attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration. 7.1.1.2.3.29. The solution shall dynamically generate real-time malware intelligence for immediate local protection via integration with the Automated Threat Correlation System. 7.1.1.2.3.30. The solution shall have the option to share dynamically generated real-time malware intelligence with a global distribution network for detecting both known malware and zero-day, highly targeted attacks used globally. 7.1.1.2.3.31. The solution shall be able to detect stealth malware both entering the network exploiting a vulnerability and communicating out to the Internet. Real-Time detection of unknown malware must be done without the use of lists & static rules. 7.1.1.2.3.32. The solution shall have automated malware analysis and accurately identify malware targeting completely unknown vulnerabilities across protocols and applications. 7.1.1.2.3.33. The solution shall be capable of blocking reliably outgoing communications to C&C servers in order to conserve data integrity on hosts including out of band infections. 7.1.1.2.3.34. The solution shall have the ability to stop data exfiltration from existing malware infected systems. 7.1.1.2.3.35. The solution shall have the ability to detect client-side EXPLOITS prior to any complex malware being downloaded to the systems; complex malware is defined as malware with complex abilities such as key-logging, data-stealing, encrypting, migrating, and installing additional complex malware. 7.1.1.2.3.36. The solution should have the ability to remain fully effective when configured to share no data, events, nor any information with vendor or the vendor's network. 7.1.1.2.3.37. The solution shall be able to deal with VM evasion techniques. 7.1.1.2.3.38. The solution shall have the capability to block Inbound Infections reliably. 7.1.1.2.3.39. The solution shall detect Zero-Day and APT attacks. 7.1.1.2.3.40. The solution shall be able to detect all three stages of the modern malware's attack lifecycle, while highlighting every stage of the attack: Exploit, Dropper & Data Exfiltration.	

	7.1.1.2.3.41. The solution shall be able to provide detailed forensic data of the actual infection, demonstrating the Full Attack Lifecycle of how the infection took place. Forensic data must include a complete timeline of the attack; web links; MD5/SHA1 hashes and actual Attached Malware binaries; any changes to Host OS; Registry; File System; & System Start-up; and chronological step-by-step of the entire attack, not solely a portion of the Attack. 7.1.1.2.3.42. The solution shall be able to utilize XFF headers to identify the client machine generating the alerts when deployed in front of a proxy server. 7.1.1.2.3.43. The solution shall utilize a Global Intelligence Network to benefit from information gathered by the research efforts of the vendor, in which subscribers receive and optionally share malware intelligence such as zero-day attacks and call-back destinations. 7.1.1.2.3.44. The solution shall have the ability to define a whitelist to exempt specific networks and/or host addresses from being blocked. 7.1.1.2.3.45. The solution shall have the ability to display the geo-location of the remote command and control server(s) when possible. 7.1.1.2.3.46. The solution shall have the ability to report the SRC IP, Destination IP, C&C, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack. 7.1.1.2.3.47. The solution shall have the ability to be deployed in the following modes: IN-LINE and SPAN / TAP 7.1.1.2.3.48. The solution shall have fail-open capability to allow all packets to pass through the sub-system in case of software, hardware or power failure when it is deployed inline. 7.1.1.2.3.49. Security Vendor shall have a Research/Laboratory organization which must contribute and report on finding new Zero-Day vulnerabilities being exploited in the wild. 7.1.1.2.3.50. To show the capability of the Security Vendor's threat research or labs team, the vendor shall have a research team which has published a paper on an APT Threat Actor. The paper should not only be focused on a specific attack, but rather focused on attribution around a specific attack group.	
	7.1.1.2.4. **Endpoint Security** 7.1.1.2.4.1. The endpoint security solution‘s monitoring agents shall be able to be controlled on and off the corporate network for the purposes of detection, triage, and containment. 7.1.1.2.4.2. The endpoint security solution’s monitoring agents shall be deployed to 15,000 endpoints within the priority agencies. 7.1.1.2.4.3. The CMS shall have solution’s monitoring agent’s visibility via GUI to monitor active and inactive agents in each agency.	

	7.1.1.2.4.4. The endpoint security solution shall be able to take as inputs custom indicators of compromise. 7.1.1.2.4.5. The endpoint security solution’s monitoring agents shall be updated automatically with most recent attacks with remediation to prevent future incidents. 7.1.1.2.4.6. The endpoint security solution shall be able to learn about zero-day threats from other security devices doing virtual execution. 7.1.1.2.4.7. The system shall be capable of isolating compromised endpoints to the attacked network with a single click on analyst dashboard via the monitoring agent. 7.1.1.2.4.8. The monitoring agents shall be capable of deploying in different Operating System (OS) such as but not limited to Windows, MAC, and Linux. 7.1.1.2.4.9. The endpoint security solution shall be able to streamline current investigative process on network and host-based alerts. 7.1.1.2.4.10. The endpoint security solution shall be able to drill into system activity during a specific incident time window to determine the source of the threat and possible data exfiltration or lateral movement. 7.1.1.2.4.11. The system shall allow near real-time malware detection, as well as capturing and recording raw data and metadata that will be useful in investigation and forensic analysis. 7.1.1.2.4.12. The system shall clearly identify endpoints that needs containment to prevent further attacks and incident to the compromised network. 7.1.1.2.4.13. The endpoint security solution shall be able to mitigate the impact of a compromised system with network isolation, killing processes, and deleting files. 7.1.1.2.4.14. The endpoint security solution shall be able to assist in an investigation in which the agent can remotely send memory dumps, files, running processes, services, drivers, DLL's, open handles, and network information. 7.1.1.2.4.15. The endpoint security solution shall include advanced exploit detection. The exploit detection shall be able to detect certain exploit activity within the process thread. Examples of exploit activity include, but are not limited to: shellcode, ROP, Heap spray, kernel exploit, or memory corruption. Exploit detection highlights abnormal process activity, which is why it can identify zero-day exploits that have not been seen before. Exploit detection does not look for a particular exploit, but rather, signs that something may be attempting to exploit a particular system.	

	7.1.1.2.4.16. The endpoint security solution shall display a snapshot of the system health information and allow health checks to be initiated from the native interface. 7.1.1.2.4.17. The endpoint security solution shall include detection of commodity malware, including items such as viruses, trojans, worms, spyware, adware, key loggers, and other potentially unwanted programs. Malware detection focuses on items which a typical anti-virus client might catch, enabling you to replace other legacy endpoint/AV solutions with a single agent. This feature should be no additional cost and a native feature from the Endpoint Detection and Response solution. 7.1.1.2.4.18. The network and endpoint security solution vendor shall have a research/labs organization and this organization must contribute and report on finding new zero-day vulnerabilities being exploited in the wild. 7.1.1.2.4.19. The network and endpoint security solution vendor shall have a research team which has published a paper on an APT Threat Actor. The paper should not be focused on a specific attack, but rather focused on attribution around a specific attack group.	
	7.1.1.2.5. **Intrusion Prevention and Detection System (IPS/IDS)** 7.1.1.2.5.1. The solution shall use a combination of technologies – including, but not limited to deep packet inspection, threat reputation, and advanced malware analysis, on a flow-by-flow basis – to detect and prevent attacks on the network. 7.1.1.2.5.2. Packet inspection and detection shall be performed and eventually block malicious web traffic on any port by IPS appliance. Accurate detection of intrusion attempts and discernment between the various types and risk levels including: unauthorized access attempts, pre-attack probes, suspicious activity, DOS, vulnerability exploitation, worms, brute force, hybrids, zero-day attacks. 7.1.1.2.5.3. The solution shall be able to run multiple Micro Tasks in a single VM (e.g. run sample across multiple versions of Adobe Acrobat in a Single VM Execution). 7.1.1.2.5.4. A separate filter, filter updates and reputation database must be supported by the IPS appliance. 7.1.1.2.5.5. The solution shall utilize hardened Virtual Machine (on-premise) technology to positively identify malware, including zero-hour vulnerability exploits, polymorphic. 7.1.1.2.5.6. The analysis in the solution shall be performed runtime in order to detect all the malware actions, even the ones that fail in the virtual environment but might be successful on a client workstation. Before and after differential comparison or VM state is not acceptable.	

	7.1.1.2.5.7. The solution shall be able to automatically generate a network communication profile if the malware tries to contact network resources during the analysis. 7.1.1.2.5.8. The solution shall provide the full malware analysis report in less than ten (10) minutes from the download. 7.1.1.2.5.9. The solution shall be able to detect and prevent advanced Malware, Zero-day attack and targeted Advanced Persistent Threat without relying on just signature database. 7.1.1.2.5.10. The solution shall have the ability to detect multi-stage attacks and must not be a file-based sandbox technology which is limited to examining one file at a time in isolation. 7.1.1.2.5.11. The solution shall automatically detect and confirm multistage zero-day malware and targeted attacks without prior knowledge of the malware. 7.1.1.2.5.12. The solution shall utilize a Global Intelligence Network to benefit from information gathered by the research efforts of the vendor, in which subscribers receive and optionally share malware intelligence such as zero-day attacks and callback destinations. 7.1.1.2.5.13. The solution's virtual execution shall be on premise as network appliances and not in the cloud. 7.1.1.2.5.14. Health monitoring of the solutions' devices, distribution of policies on a schedule or on-demand basis, generation of scheduled automatic and manual reports and back-up the solution's filter configuration must be done and shown on console of the management device	
	7.1.1.2.6. **Application Delivery Controller (ADC)** 7.1.1.2.6.1. The solution shall be full proxy load-balancing and context-switching solution. 7.1.1.2.6.2. The solution shall be able to determine health of physical servers with customizable server health check. 7.1.1.2.6.3. The solution shall have service delivery acceleration using TCP connection multiplexing, RAM caching, compression, SSL offload, expedited content transfer. 7.1.1.2.6.4. The solution shall support multitenant environment. 7.1.1.2.6.5. The solution shall support the following deployment options: One Arm Deployment, Inline Deployment, Dual Stack Ipv4/Ipv6 and Transparent Mode/Gateway Mode and High Availability Architecture Support for Active-Active and Active-Standby 7.1.1.2.6.6. The solution shall be able to do Caching and Compression. 7.1.1.2.6.7. The solution shall a built-in WAF with capability to do DNS or non-DNS based site to site load balancing. 7.1.1.2.6.8. The solution shall have the following comprehensive load balancing methods: 7.1.1.2.6.8.1. Round Robin	

	7.1.1.2.6.8.2. Weighted Round Robin 7.1.1.2.6.8.3. Least request 7.1.1.2.6.8.4. Least connection per server level 7.1.1.2.6.8.5. Least connection per service port level 7.1.1.2.6.8.6. Server Ratio, Weighted Least connection 7.1.1.2.6.8.7. Fastest response on service port level 7.1.1.2.6.8.8. Server priority 7.1.1.2.6.9. The solution shall be able to support Dynamic Routing Protocol and the following Routing Protocols: Static Routes, IS-IS (v4-v6), RIPv2/ng, OSPF v2/v3 and BGP4+. 7.1.1.2.6.10. The solution shall support for VLAN (802.1Q) and Trunking (802.1AX), LACP 7.1.1.2.6.11. The solution shall support for Traditional IPv4-->IPv4 NAT/NAPT and IPv6-->IPv6 NAPT 7.1.1.2.6.12. The solution shall have dedicated management interface (Console, SSH, Telnet, HTTPS), Command Line Interface (CLI) support and Web-based Graphical User Interface (GUI) with Language Localization 7.1.1.2.6.13. The solution shall have integration support for LDAP, TACACS+, RADIUS, SNMP, Syslog, email for notification 7.1.1.2.6.14. Must have REST-style XML API support, TCL Scripting Support and Symmetric Multi-Processing Support 7.1.1.2.6.15. Must have Hot Swap Redundant Power Supplies (AC or DC)	
	7.1.1.3. Monitoring Tools 7.1.1.3.1. **Network Monitoring** 7.1.1.3.1.1. The internal and external monitored traffic shall be at minimum of 1Gbps on each priority agency. 7.1.1.3.1.2. The solution shall be able to consume external threat intelligence feeds to enrich monitoring data. 7.1.1.3.1.3. The solution shall compare the payload of the CMSP monitored network traffic to the malicious hashes received in the intelligence feeds. 7.1.1.3.1.4. The solution shall be able to monitor multiple 1GE links in a passive, non-intrusive manner. 7.1.1.3.1.5. The solution shall be able to aggregate multiple 1GE links to one 1GE interface to increase the throughput of the links in a passive, non-intrusive manner. 7.1.1.3.1.6. The solution shall detect anomalies on network traffic. 7.1.1.3.1.7. The solution shall detect zero day attacks or exploit. 7.1.1.3.1.8. The solution shall be able to tag aggregate links using IP address ranges or VLAN tagging to allow identifying from which source a specific traffic arrived.	
	7.1.1.3.2. **Detection Sensors** 7.1.1.3.2.1. The solution shall support White List, Black List, and Neutral List to optimize detection by lowering false positives:	

	7.1.1.3.2.2. Black List – network identifiers that should always generate alert. 7.1.1.3.2.3. White List – network identifiers that should never generate alert. 7.1.1.3.2.4. Neutral List – network identifiers that should not be in the Black or White Lists (alert will pop).	
	7.1.1.3.3. **Vulnerability and Malicious File Detection** 7.1.1.3.3.1. The solution shall be able to inspect incoming, through web, email and file streams, and detect at least the following without relying on signatures: exploits in documents, zero-day vulnerabilities, injected code and processes, DLL injection, shell code. 7.1.1.3.3.2. The solution shall be able to conduct file analysis on office documents, open office documents, PDF, archives, and password-protected files. 7.1.1.3.3.3. The solution shall use multiple scan engines, and these engines will be used subsequently. 7.1.1.3.3.4. The solution shall use the results received from each engine and utilize this information in the subsequent engines and the system will know how to utilize the results. 7.1.1.3.3.5. The solution shall know how to aggregate the results of all the scan engines into one comprehensive report. 7.1.1.3.3.6. The solution shall be able to conduct static file analysis within sub-second per file and scalable to hundreds of thousands of files a day with the provided hardware and software set. 7.1.1.3.3.7. The solution shall be resilient to anti-sandboxing evasion techniques such checking for virtual context or for hooking, waiting for user interaction, waiting extended period. 7.1.1.3.3.8. The solution shall use cache results and threat intelligence to prevent redundant scans of identical files. 7.1.1.3.3.9. The solution shall use scanning profiles that allow optimizing performance and security coverage, including real time detection and on demand scans. 7.1.1.3.3.10. The solution shall be able to extract a malicious payload from documents files and examine the payload in virtual execution environment and identify IOC in the payload. 7.1.1.3.3.11. The solution shall be able to validate and provide accurate evidence to every vulnerability. 7.1.1.3.3.12. The solution must automatically map a vulnerability to a known public exploit if available. 7.1.1.3.3.13. The solution shall be able to provide asset inventory of the organization. 7.1.1.3.3.14. The solution shall have task scheduling capabilities. 7.1.1.3.3.15. The solution shall have visual analytics and dashboarding capabilities.	

7.1.1.3.4. **Command and Control (C&C) Detection**

7.1.1.3.4.1. The solution shall be able to detect malware attacks already inside the organization network.

7.1.1.3.4.2. The solution shall be able to detect command and control channels, using network monitoring.

7.1.1.3.4.3. The solution shall address new and unknown malware threats. Specifically, it shall not rely on solely signatures or rules (neither provided by vendor, nor maintained by customer), and must leverage behavioral analysis and machine learning.

7.1.1.3.4.4. The solution shall leverage big data techniques in the detection process.

7.1.1.3.4.5. The solution shall include, out of the box, a robust set malware classifiers and detection models that are comprehensive enough to be effective upon deployment.

7.1.1.3.4.6. The solution shall include self-learning capabilities whereby the detection classifiers and models adjust themselves to the surveyed organization network.

7.1.1.3.4.7. The solution shall include and leverage reputation lists of known C&C servers.

7.1.1.3.4.8. The solution shall include C&C evasion techniques over DNS manipulation including Domain Generation Algorithm (DGA).

7.1.1.3.4.9. The solution shall use and consider in calculation large number of different indicators on traffic examined.

7.1.1.3.4.10. The solution shall classify in its detection process the malware related family or malware similarity to other known malware types, and the system is capable on how to detect such.

7.1.1.3.4.11. The solution shall provide confidence scoring to help analysts understand and assess the traffic classified from the detectors.

7.1.1.3.4.12. The solution must be able to detect advanced Malware, Zero-day attack and targeted Advanced Persistent Threat without relying on just Signature database

7.1.1.3.4.13. The solution must support dynamic real-time analysis of advanced malware to confirm true zero-day and targeted attacks.

7.1.1.3.4.14. The solution must have the ability to detect multi-stage attacks and must not be a file based Sandbox technology which is limited to examining one file at a time in isolation

7.1.1.3.4.15. The solution must have real-time malware intelligence with a global distribution network for detecting both known malware, zero-day, and highly targeted attacks used globally.

7.1.1.3.4.16. The solution must have the ability to report the Src IP, Destination IP, C&C, URL, Malware family or class,

	executables, used protocols and infection severity of the attack.	
	7.1.1.3.5. **Lateral Movement Detection** 7.1.1.3.5.1. solution shall apply invisible network-based inspection to detect internal reconnaissance and lateral movement attempts within the organization network. 7.1.1.3.5.2. The solution shall detect lateral movement propagation attempts between endpoints. 7.1.1.3.5.3. The solution shall detect post-exploitation, credential, harvesting attack, etc. 7.1.1.3.5.4. The solution shall leverage passive LAN traffic sniffing, to simplify deployment and to be invisible to attacker. 7.1.1.3.5.5. The solution must have a correlation engine that analyses and correlates lateral movement attacks from disparate sources and generates alerts when post-infection attacker activity is detected.	
	7.1.1.3.6. **Log Collection and Correlation** 7.1.1.3.6.1. The solution shall receive logs to SOC's internal chosen perimeters such as Firewall, A/V etc. 7.1.1.3.6.2. The solution shall also be deployed in the SOC's ten (10) priority agencies. The agencies are DICT, NSC, DND, DFA, PCOO, OP/PMS, DOE, DBM, DOF and NICA. 7.1.1.3.6.3. The solution shall support collection through standard syslog or JSON protocol. 7.1.1.3.6.4. The solution should be scalable and capable to accommodate unlimited storage. 7.1.1.3.6.5. The solution shall receive logs from covered site's chosen perimeter security tools (e.g. Firewalls, AVs) via dedicated log collectors, deployed at each site. 7.1.1.3.6.6. The solution shall be able to receive alerts via syslog or JSON. 7.1.1.3.6.7. The solution design and data should be designed to allow quick access to terabytes of historical data. It should be able to provide very fast and distributed searching. 7.1.1.3.6.8. It solution shall be able to ingest all the original, unmodified data and make it searchable (no data reduction). 7.1.1.3.6.9. The solution shall comply with a globally accepted cyber security compliance standard/s. 7.1.1.3.6.10. The solution shall provide real-time monitoring of the events and raw logs of the organizations security posture. 7.1.1.3.6.11. The solution shall be able to maintain the original timestamps for each event while handling timestamps from different timezones. 7.1.1.3.6.12. It should be able to create data stores summarizing raw data, and then run searches/reports on these summaries for faster performance.	

	7.1.1.3.6.13. The solution shall have ad hoc searches for faster collection of evidence to incidents. 7.1.1.3.6.14. The data retention settings shall be flexible as follows: Can retain ingested data as long as desired: Days, months, or years, Granular control on what happens to data as it ages. Aged data can be rolled off to external/cheaper storage and/or deleted. 7.1.1.3.6.15. The solution should be able for replication to maintain multiple, identical copies of ingested data for data availability, data fidelity, disaster tolerance, and improved search performance. 7.1.1.3.6.16. The solution shall be integrated easily with any third-party, free or commercial, human readable threat intelligence feed.	
	7.1.1.4. Management Tools 7.1.1.4.1. The solution shall provide case management capabilities (e.g. user assignments, incident workflow, etc.) 7.1.1.4.2. The solution shall support segregation method per analyst and customization of user privilege in the SOC. 7.1.1.4.3. The solution shall support dashboard for active case summary, security performance, and SOC team performance. 7.1.1.4.4. The solution shall provide online ticketing capabilities and supports the following incident status types: Open, Close, Resolved, and Unresolved. 7.1.1.4.5. The solution shall present the incident workflow via dashboard. 7.1.1.4.6. The solution shall present a summary report to the SOC manager showing the severity and total number of incidents. 7.1.1.4.7. The solution shall support creation of case from one or more alerts. Relevant information including links to the alert(s) shall also be provided. 7.1.1.4.8. The solution shall support incident documentation - both automated and manual steps.	
	7.1.1.5. Artificial Intelligence (AI) / Machine Learning 7.1.1.5.1. **Automated Analysis** 7.1.1.5.1.1. The solution shall be able to analyze and evaluate alerts coming into the SOC network. 7.1.1.5.1.2. The solution shall be able to analyze anomalies on network traffic from behaviour of users, devices on the network, and zero day threats. 7.1.1.5.1.3. The solution shall be able to analyze unusual and unauthorized behaviour within the network such as port scanning, unauthorized plugged in, and unauthorized use of access credentials to internal resources. 7.1.1.5.1.4. The solution shall be capable of analysing unusual web traffic, unique IP addresses and shall detect data exfiltration and unusual data transfers.	

	7.1.1.5.1.5. The solution shall include capability for human analysts to assign if the alerts were True Positive or False Positive. 7.1.1.5.1.6. The solution's GUI shall represent the behaviour of alerts for the visualization and analysis of the user. 7.1.1.5.1.7. The solution's GUI shall have a "play back" feature that allows user to go back to a specific date and time where the analysis was made for investigation purposes. 7.1.1.5.1.8. The solution shall categorize the type of alert received by the SOC whether it is a threat data or a cybercrime such as fraud and identity theft.	
	7.1.1.5.2. **Automated Investigation** 7.1.1.5.2.1. After the analysis of alerts, real attacks shall automatically be included in the SOC incident queue. 7.1.1.5.2.2. The solution shall allow authorized users in the SOC to have an access to all incidents to allow full transparency. 7.1.1.5.2.3. The solution shall be able to recommend analysts which incidents can be merged with other related incidents and which incidents can be closed. 7.1.1.5.2.4. The solution shall be able to automate at least certain steps in incidents enrichments and evidence gathering, including, but not limited to the following enrichment capabilities: Threat Intelligence, Reputation Feeds, IP-Geolocation. 7.1.1.5.2.5. The solution shall include investigative tips to the human analyst for investigating an alert. 7.1.1.5.2.6. The solution shall provide GUI representation of entities and relationships that are extracted from alerts and incidents for a faster investigation and evidence gathering. 7.1.1.5.2.7. The solution shall allow specified analyst to hunt for unknown / undetected malware by enabling them full access to incidents, alerts, and raw data that was monitored in the SOC. 7.1.1.5.2.8. The entire investigation process, findings and rationale must be documented in a workflow steps format, whether steps were conducted automatically or by human analyst, as to present the analysis carried so far. 7.1.1.5.2.9. The entire investigation process, findings and rationale must be documented in a workflow steps format, whether steps were conducted automatically or by human analyst, as to present the analysis carried so far. 7.1.1.5.2.10. The solution shall generate visual analysis that shows the connection and entities involved in the incident for further investigation of the human analyst. 7.1.1.5.2.11. The solution shall generate summary of findings and recommendation to incident. 7.1.1.5.2.12. The solution shall allow sharing of incident journal / notes between human analyst.	

	7.1.1.5.3. **Threat Profiling** 7.1.1.5.3.1. The solution shall generate summary profile of an entity base on the data extracted from the incident. 7.1.1.5.3.2. The solution shall include the following data in generating summary profile of entities: 7.1.1.5.3.2.1. IP Address 7.1.1.5.3.2.2. Executable and non-executable files 7.1.1.5.3.2.3. Compromised Endpoints 7.1.1.5.3.2.4. Compromise emails and SMTP address 7.1.1.5.3.2.5. Entity behaviour and processes 7.1.1.5.3.3. The solution shall include GUI representation of the incident flow and behaviour profile of the entity.	
	7.1.1.5.4. **Dark Web Investigation** 7.1.1.5.4.1. The solution shall collect automatically TOR information for more than 3,000 onion URLs. Information should be added at least on an hourly based. 7.1.1.5.4.2. The solution shall support searches and analysis in multiple languages. 7.1.1.5.4.3. The solution shall provide filtering capability such as, but not limited to date, categories, authors, etc. 7.1.1.5.4.4. The solution shall provide Boolean keywords filtering. 7.1.1.5.4.5. The solution shall provide searching parameters such as, but not limited to: Title and Content 7.1.1.5.4.6. The solution shall be capable to alert by email if any related information is discovered/collected from a case of interest. 7.1.1.5.4.7. The solution shall be able to show results and is capable to be presented into list and charts. 7.1.1.5.4.8. The solution shall enable content filtering by content, such as, but not limited to: Chat, Post, Reply, Feedback. 7.1.1.5.4.9. The solution shall be able to provide profile analysis of authors including: 7.1.1.5.4.9.1. Popularity in forum. 7.1.1.5.4.9.2. Actor's alias(es) in other forum. 7.1.1.5.4.9.3. Link Analysis on darkweb 7.1.1.5.4.9.4. Activity Analysis panel to displays the actor's work pattern on a 24 by 7 matrix 7.1.1.5.4.9.5. Categories shall give an indication of the actor's area 7.1.1.5.4.10. The solution’s case management shall allow users to create insights. 7.1.1.5.4.11. The solution shall allow users to add comments / flag topics. The solution shall enable users to manually input information of interest into cases. 7.1.1.5.4.12. The solution shall support the exporting of a case to a Word document / CSV files with Comments, Saved Posts, Actors, Social Network.	

	7.1.1.5.4.13. The solution shall enable the sharing of cases, searches and posts with other users of the platform. 7.1.1.5.4.14. The solution shall have a responsive and rich GUI which enables the user to use the tool efficiently. 7.1.1.5.4.15. The solution shall not require the user to wait for collection of the information to start the investigation, as the applicable data will already reside within the platform DB. 7.1.1.5.4.16. The solution shall be embedded with the following relevant intelligence: 7.1.1.5.4.16.1. Baseline Cyber Threat Intelligence Report 7.1.1.5.4.16.2. Ontologies – Ransomware, Data leak, Exploit, Malware, Financial fraud, etc. 7.1.1.5.4.16.3. Cases 7.1.1.5.4.16.4. Avatars	
	7.1.1.5.5. **Forensics** 7.1.1.5.5.1. Network Forensics - The solution shall allow monitoring and analysis of computer network traffic for the purpose of investigation. 7.1.1.5.5.2. The recorded data shall enable the analyst to confirm incidents and alerts. As well as understand the nature, scope and damage that was already done. 7.1.1.5.5.3. The solution shall be able to construct and understand view of attacks, its scope and impact to the organization. 7.1.1.5.5.4. The solution shall be able to understand where the source of attack, its behaviour, and method used in the attack. 7.1.1.5.5.5. The solution shall be able to gather evidence required to contain and remediate the attack. 7.1.1.5.5.6. The solution shall have a retention period of thirty (30) days. 7.1.1.5.5.7. The solution shall be able to capture both external and internal traffic. 7.1.1.5.5.8. The solution must support continuous and lossless packet capture with nanosecond time stamping at recording speeds up to 20 Gbps. 7.1.1.5.5.9. The solution shall index the recorded data that includes source and destination IP address/port number, and protocol. 7.1.1.5.5.10. The solution shall enable queries based on both endpoint hostnames and IP addresses.	
	7.1.1.5.5.11. Endpoint Forensics 7.1.1.5.5.11.1. The solution shall support up to 1500 endpoints at each covered organization. 7.1.1.5.5.11.2. The solution shall support continuous Endpoint forensics capabilities at kernel-level, including running processes, files, registries, logs, etc., for analyst investigations.	

	7.1.1.5.5.11.3. The solution shall provide report readable to human analyst for the conduct of retroactive inspection and investigation of suspicious entities. 7.1.1.5.5.11.4. The solution shall provide reports 7.1.1.5.5.11.5. The endpoint forensic scan must support different types of operating system such as but not limited to Windows, MAC OS, and Linux 7.1.1.5.5.11.6. The solution shall be able to enrich its endpoint forensics results with other incident data.	
	7.1.1.5.6. **Response System** 7.1.1.5.6.1. Actionable Intelligence 7.1.1.5.6.1.1. The solution shall be able to provide actionable intelligence to allow remediating current attack and prevent recurring of attacks. 7.1.1.5.6.1.2. The solution shall be able to escalate the incidents to proper organization or agency. Cybercrime incidents should be forwarded to Law Enforcement Agencies while breach or cyber-attacks shall retain in the SOC for further investigation. 7.1.1.5.6.1.3. The solution shall provide recommendations and patch management reports to every Vulnerabilities detected by the threat intelligence feeds. 7.1.1.5.6.1.4. The solution shall manually create rules based on the investigation outcome.	
	7.1.1.5.7. **Reports** 7.1.1.5.7.1. The solution shall have 1 click incident report mechanism with detailed attack chronology, scope, evidences collected and remediation steps required or taken. The report must be available as part of the browser-based GUI and also exportable to PDF format. 7.1.1.5.7.2. The solution shall provide periodic report showing aggregated and statistical data for the protected organization for the given period, including attacks, incidents, alerts, and system performance data. 7.1.1.5.7.3. The solution shall automatically generate and send bulletin report of about the most recent cyber-attacks with recommendations to the department, priority agencies, and all government agencies that may be affected by the cyber threats. 7.1.1.5.7.4. Each report shall include Summary of the revealed vulnerabilities and treats, in depth analysis of the threat, and Remediation recommendation. 7.1.1.5.7.5. The report shall contain current status of attacks or incidents in local and international community. 7.1.1.5.7.6. The solution shall automatically generate summary reports to the C-level managers.	

	7.1.1.5.7.7. The system shall include monitoring and reporting system of each security perimeter with physical status, storage, and systems functionality in the dashboard to quickly respond and prevent potential problems in the hardware and other SOC's security perimeter.	
	7.1.1.6. Portable CMS 7.1.1.6.1. The solution shall include a minimum of one (1) portable CMS solution. 7.1.1.6.2. The solution shall be mobile and can be easily deployed to different agencies in case of emergency which can also monitor, detect and respond to incident. 7.1.1.6.3. The solution shall be easy to use and self-sufficient that can be connected any network. 7.1.1.6.4. The solution shall generate results within hours. 7.1.1.6.5. The solution shall perform quick incident response to organizations that is under real-time cyber-attack. 7.1.1.6.6. The solution shall allow investigation of breaches regardless of security or logging tools in place. 7.1.1.6.7. The solution shall include operational capability of the main SOC such as detection, investigation, forensics, and response tools to support variety of incidents. 7.1.1.6.8. The solution shall generate actionable intelligence to allow remediation of incidents. 7.1.1.6.9. The solution shall have at least two (2) weeks of forensics retention. 7.1.1.6.10. The solution shall be capable of incident response without unnecessary disruption of vital operations of the agency / organization.	
	7.1.1.7. Disaster Recovery Management System 7.1.1.7.1. The Vendor shall provide disaster recovery site for the SOC. 7.1.1.7.2. The backup storage shall be a stand-alone storage SAN appliance, connected to the CMS. 7.1.1.7.3. The solution shall include a dedicated Backup storage appliance that will serve as a backup to the CMS central storage. The backup storage shall be capable of storing in a remote site. 7.1.1.7.4. The CMS shall be implemented over a Virtualized environment (VM), connected to a central storage appliance. The backup function shall be implemented on the CMS central storage appliance. 7.1.1.7.5. The CMS Central storage shall be replicated to the solutions' backup storage appliance, which will serve as a backup for the whole CMS central storage data. In case of emergency or failure of operation, the backup and restore function shall enable retrieval of the entire CMS data and operations.	

7.1.1.7.6. The solution's storage device shall be configured with a recurring snapshot policy and a percentage of storage allocated for snapshot reserve (according to the required backup retention).

7.1.1.7.7. Upon storage corruption the storage shall enable restoring the system data from a selected snapshot, which is closest to the time of storage failure / data corruption.

7.1.1.7.8. The backup function, produced by the storage device vendor, shall run on the storage device. There will be no need to install backup SW on the SOC system servers.

7.1.1.7.9. The solution's backup storage shall store backup data for six (6) months. It must be expandable to support three (3) years growth with fifty (50) agencies connected to the main CMS site, each with 1500 endpoints.

1st year	2nd year	3rd year
10 Agencies	20 Agencies	20 Agencies

7.1.1.7.10. The initial Backup storage size shall be at least 13 Terabyte net storage.

7.1.1.7.11. The backup storage shall backup data from the central CMS site. The data shall include:

7.1.1.7.12. CMS Virtual Machines SW and configuration files

7.1.1.7.13. CMS database, including the system alerts and investigations

7.1.1.7.14. Upon failure of a server in the SOC, a replacement server shall retrieve the failed server SW and data from the storage appliance to resume the failed server functionality.

7.1.1.7.15. The storage SAN appliance vendor shall be a major vendor in the market (e.g. EMC, NetApp).

7.1.1.7.16. The solution shall have the capability to support and continue the main SOC's operation in case of disaster or emergency.

7.1.1.7.17. The DR management system shall include real-time backup and power management in case of emergency.

7.1.1.8. Storage

7.1.1.8.1. Data Lake

7.1.1.8.1.1. The solution shall be integrated in the SIEM to support the number of incoming logs in the central CMS.

7.1.1.8.1.2. The solution shall have a retention period of sixty (60) days.

7.1.1.8.1.3. The solution shall be able to support the SIEM in collecting logs from the priority agencies.

7.1.1.8.1.4. The solution platform shall take a scale-out approach, accommodating increasing volumes and support a full read/write file system.

7.1.1.9. Vulnerability Assessment and Penetration Testing (VA/PT) Tool

7.1.1.9.1. The solution shall have at least a 3 GHZ+ processor.

7.1.1.9.2. The solution shall include at least 32GB RAM and 256 SSD x 3 GB available disk space which increases with VM target on a certain device.

7.1.1.9.3. The solution shall support the following operating systems:

7.1.1.9.3.1. Ubuntu Linux 14.04 or 16.04 LTS (RECOMMENDED)

7.1.1.9.3.2. Microsoft Windows Server 2008 R2

7.1.1.9.3.3. Microsoft Windows Server 2012 R2

7.1.1.9.3.4. Microsoft Windows 10

7.1.1.9.3.5. Microsoft Windows 8.1

7.1.1.9.3.6. Microsoft Windows 7 SP1+

7.1.1.9.3.7. Red Hat Enterprise Linux Server 7.1 or later

7.1.1.9.3.8. Red Hat Enterprise Linux Server 6.5 or later

7.1.1.9.3.9. Red Hat Enterprise Linux Server 5.10 or later

7.1.1.9.3.10. Kali Linux

7.1.1.9.4. The solution shall support the latest versions of the following web browsers:

7.1.1.9.4.1. Google Chrome

7.1.1.9.4.2. Mozilla Firefox

7.1.1.9.4.3. Microsoft Explorer

7.1.1.9.5. The solution shall be able to connect and operate with physical hardware in an effort to perform security testing on non-ethernet based systems.

7.1.1.9.6. The solution shall validate and provide evidence to scanned vulnerabilities.

7.1.1.9.7. The solution shall automatically adjust its scans' intensity according to how devices react, to avoid overloading them with scan traffic.

7.1.1.9.8. The solution shall be able to scan internal and external IP's.

7.1.1.9.8.1. Shall support scanning IPv4 and IPv6

7.1.1.9.8.2. Shall allow scan by hostname

7.1.1.9.8.3. The solution shall use proper asset tracking like IP based, DNS or NetBIOS hostname based

7.1.1.9.8.4. The solution shall be available in hardware and a virtual appliance version

7.1.1.9.8.5. Hardware scanners must have fast disks like SATA and bigger storage like ~ 1TB

7.1.1.9.9. The solution shall perform authenticated scans and null session scans.

7.1.1.9.10. The solution shall have minimal or no impact on Network traffic, server performance, network devices etc. during deployment and operation.

7.1.1.9.11. The solution shall provide encrypted data at transmission between the scanner and the organizations engine.

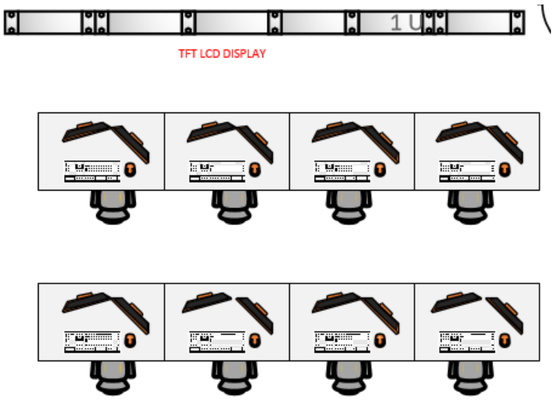
7.1.1.9.12. The solution shall have inventory capabilities to OS, assets, ports and services, applications, users on the system.

	7.1.1.9.13. The solution shall allow searching in the inventory. Searching should be fast and accurate. 7.1.1.9.14. The solution shall provide scanned history information including the last scan date of an asset in the inventory view. 7.1.1.9.15. The solution shall be scalable 7.1.1.9.16. The solution shall support up to 15000 endpoints (1500 per agency) 7.1.1.9.17. The solution shall include subscription up to three (3) years. 7.1.1.9.18. The solution shall be able to conduct vulnerability assessment for all major operating systems and their versions including but not limited to: Windows, AIX, Unix, Linux, Solaris, OSX, IOS. 7.1.1.9.19. The solution shall provide alerts for vulnerabilities, ports, certificates, software installed. 7.1.1.9.20. The solution shall allow multiple scan jobs at the same time 7.1.1.9.21. The solution shall identify presence of Load balancers, firewalls or other L3 devices during scan. 7.1.1.9.22. The solution shall provide Real-Time Correlation of Active Threats Against Vulnerabilities detected in the environment 7.1.1.9.23. Scan must be able to include or exclude a specific list of signatures 7.1.1.9.24. The solution shall have inbuilt reporting templates 7.1.1.9.25. The solution shall allow custom template creation 7.1.1.9.26. The solution shall allow various output formats like CSV, DOC, HTML, PDF, XML etc. 7.1.1.9.27. The solution shall allow to report NEW, ACTIVE, FIXED or RE-OPENED vulnerabilities. 7.1.1.9.28. The solution shall report on First found date, last found date and number of times detected. 7.1.1.9.29. The solution shall not allow anyone except the template owners to make changes to the template. 7.1.1.9.30. The solution's reporting system shall filter out superseded patches. 7.1.1.9.31. The scanners shall have vertical and horizontal growth to support scaling and redundancy. 7.1.1.9.32. Scanner device (hardware/software) shall be self-updating. 7.1.1.9.33. The solution shall have a good enough uptime, scalability and security.	
	7.1.1.10. Network Infrastructure 7.1.1.10.1. Network Switch 7.1.1.10.1.1. Provide 24 10/100/1000BASE-T POE+, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+ 7.1.1.10.1.2. Support external redundant power supply. 7.1.1.10.1.3. Provide up to 128Gbps switch bandwidth and 95.2Mpps frame forwarding rate.	

	7.1.1.10.1.4. Upgradeable uplink ports from 1G to 10G (Need 10G port license) 7.1.1.10.1.5. The switch operating system must be highly resilient and modular. 7.1.1.10.1.6. The switch operating system must allow the upgrading of individual software modules and restart unresponsive process. 7.1.1.10.1.7. The switch operating system must support self-healing process recovery via process restart. 7.1.1.10.1.8. Support use of same switch operating system image across the proposed access switches models for ease of management. 7.1.1.10.1.9. Support IEEE 802.3af and 802.3at standard (Power over Ethernet) 7.1.1.10.1.10. Support 802.3ad Link Aggregation, 802.1w RSTP, 802.1s MSTP and PVST+. 7.1.1.10.1.11. Support up to 128 load sharing trunks, up to 8 members per trunk. 7.1.1.10.1.12. Support up to 4000 Port-based or Protocol-based or 802.1Q or 802.1ad VLANs. 7.1.1.10.1.13. Support Private VLAN, VLAN Translation. 7.1.1.10.1.14. Can support VLAN Aggregation. (Advanced License) 7.1.1.10.1.15. Support IP static routing, RIPv1/v2 routing features. 7.1.1.10.1.16. Can support 4 active OSPF interfaces. (Advanced License) 7.1.1.10.1.17. Support Equal Cost Multi Path for IPv4 and IPv6. 7.1.1.10.1.18. Can support PIM-SM Edge, PIM-SSM Edge and static multicast routing. (Advanced Edge License) 7.1.1.10.1.19. Can support VRRP and VRRPv3. Virtual Router Redundancy Protocol (VRRP) enables a group of routers to function as a single virtual default gateway to provide gateway redundancy for users. (Advanced Edge License) 7.1.1.10.1.20. Support IPv6 static routing and RIPng. 7.1.1.10.1.21. Can support 4 active OSPFv3 interfaces. (Advanced Edge License) 7.1.1.10.1.22. Provide following IPv6 features: 7.1.1.10.1.22.1. IPv4 and IPv6 dual stack and DNS client. 7.1.1.10.1.22.2. Ping, Traceroute, Telnet and SSH-2 7.1.1.10.1.22.3. ICMPv6 and Neighbor Discovery 7.1.1.10.1.22.4. Stateless Address Auto Configuration 7.1.1.10.1.22.5. DHCPv6 Relay 7.1.1.10.1.22.6. IPv6 Access Control List 7.1.1.10.1.22.7. RA (Router Advertisement) Filtering 7.1.1.10.1.22.8. Provide RFC 6106 DNS option for Router Advertisement. 7.1.1.10.1.22.9. 6to4 Tunnel and 6in4 Tunnel. (Optional via software license)	

	7.1.1.10.1.23. Support ITU-T G.8032 Ethernet Ring Protection Switching or equivalent with sub-second recovery. 7.1.1.10.1.24. The switch operating system must support scripting capability to allow automating regular management tasks in scripts and deploy configurations such as QoS, rate limiting and ACLs. 7.1.1.10.1.25. Support framework of event-driven activation of CLI scripts which can leverage any system event log message as an event trigger, the most popular use cases are time/user/ location-based dynamic security policies as well as VoIP auto-configuration. 7.1.1.10.1.26. Support Kerberos snooping to work with Microsoft Active Directory to allow access and track users in the network. The switch can retrieve IP, MAC, VLAN, computer hostname, and port location of the user. 7.1.1.10.1.27. Support sFlow or Netflow. 7.1.1.10.1.28. Support a framework for implementing security, monitoring, and anomaly detection. The framework allows you to specify certain types of traffic that require more attention. After certain criteria for this traffic are met, the switch can either take an immediate, predetermined action, or send a copy of the traffic off-switch for analysis. 7.1.1.10.1.29. Support 802.1ag L2 Ping and traceroute, Connectivity Fault Management 7.1.1.10.1.30. Support ITU-T Y.1731 Frame delay measurements 7.1.1.10.1.31. Support SNMP v1/v2/v3, RMON, SMON, XML management interfaces. 7.1.1.10.1.32. Support Network Time Protocol server and Client. 7.1.1.10.1.33. Support IEEE 802.1AK Multiple Registration Protocol and Multiple VLAN Registration Protocol to share VLAN information and configure the needed VLANs dynamically within a layer 2 network. 7.1.1.10.1.34. Can support 802.1BA AVB to enable reliable, real-time audio/ video transmission over Ethernet for today's high-definition and time-sensitive multimedia streams with perfect Quality of Service (QoS). (AVB Multi-Media Feature Pack) 7.1.1.10.1.35. Can support OpenFlow to provide an external OpenFlow based SDN controller to access and control the forwarding plane of the switch. (SDN-OpenFlow Feature Pack) 7.1.1.10.1.36. Support up to 4 mirroring instances. A mirroring instance consists of a unique destination port(s) and source port(s). 7.1.1.10.1.37. Support Heterogeneous Stacking feature 7.1.1.10.1.38. Support following stacking mechanism:	

	7.1.1.10.1.38.1. Up to 8 switches in a stack 7.1.1.10.1.38.2. Support stacking with 10GE switches 7.1.1.10.1.38.3. n-1 master redundancy 7.1.1.10.1.38.4. Distributed Layer 2 and Layer 3 switching 7.1.1.10.1.38.5. 50 milliseconds failover. 7.1.1.10.1.39. Support the ability to authenticate multiple users on a single port via 802.1X, Web or MAC at the same time. 7.1.1.10.1.40. Support dynamic role-based policy, independent of the VLAN assigned to the port, to secure and provision network resources based upon the role the user or device plays within the network. 7.1.1.10.1.41. Provide up to 48 x 1Gb/10Gb SFP+ ports with 2 x 10Gb/40Gb QSFP+ ports and Up to 4 x 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports switch model. 7.1.1.10.1.42. Provide up to 48 x 1Gb/10Gb 10GBase-Tx ports with 2 x 10Gb/40Gb QSFP+ ports and Up to 4 x 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports switch model. 7.1.1.10.1.43. Provide system performance of at least 1.76Tbps Switching Capacity 7.1.1.10.1.44. The switch operating system must be highly resilient and modular. 7.1.1.10.1.45. The switch operating system must allow the installing or upgrading of individual software modules and restart unresponsive process. 7.1.1.10.1.46. The switch operating system must support self-healing process recovery via process restart. 7.1.1.10.1.47. Provides Private VLAN, VLAN Translation, and VLAN Aggregation. 7.1.1.10.1.48. Provide static route, RIPng and Policy Based Routing for IPv6. 7.1.1.10.1.49. Able to support full OSPFv3, IS-IS and BGP4+ for IPv6. (Core License) 7.1.1.10.1.50. Provide RFC 3619 Ethernet Automatic Protection Switching (EAPS). 7.1.1.10.1.51. Provide ITU-T G.8032 Ethernet Ring Protection Switching (ERPS) to enable carrier grade resiliency. 7.1.1.10.1.52. Provide IEEE P802.1Qaz DCBX (Data Center Bridging eXchange) to exchange configuration information with directly connected peers. 7.1.1.10.1.53. OpenFlow based SDN controller to access and control the forwarding plane of the switch. (Optional SDN-OpenFlow Feature Pack)	
8.	**Other Physical Parameters**	
	8.1. Console Desk System	

	8.1.1. Two (2) Clusters where each cluster is for 4 SOC operators with 24" Dual LCD monitor 8.1.2. Total length should be not less than 5.300meters, height should be not lower than .725meters 8.1.3. Each cluster console should be identical and should have the following specs: 8.1.3.1. Modern contemporary and minimalist look and feel 8.1.3.2. Free seating concept. SOC operators can seat anywhere and still have access to assigned workstation PC 8.1.3.3. Ergonomic and modular 8.1.3.4. Worktop: minimum 20mm thick phenolic to withstand better heat and humidity and in duck nose front edging 8.1.3.5. Built-in drawers in 1.2mm thick cold rolled steel and in phenolic laminate front doors 8.1.3.6. Terminal panels for mounting Power Strips, etc. should be not less than 1.2mm thick Cold Rolled Steel 8.1.3.7. Horizontal Profile should be extruded aluminum 8.1.3.8. Should include aluminum Ergonomic LCD Arm for dual monitor 8.1.3.9. Modular Design (ability to accommodate future upgrade / relocation)	
	8.2. Submission Requirement 8.2.1. Proposed console design should include detailed dimensions and specifications and materials in 2D such as top-view, cross section and side view. 8.2.2. Proposed console design drawing should include ergonomic operator viewing to conform with Ergonomics 8.2.3. Proposed console design should include 3D rendered drawing	
	8.3. Console Layout  **Figure 11.3 Console Layout Design**	
	8.4. Video wall Display **8.4.1.** System Specifications 8.4.1.1. Include installation, configuration, testing and commissioning 8.4.1.2. 2 x 4 configuration videowall display	

	8.4.1.3. Branded 55" Full HD led-LCD Display (Industrial Grade) 8.4.1.4. Bezel-to-bezel gap: 1.25 mm 8.4.1.5. Brightness: 500 8.4.1.6. Connections Input: HDMI, DP, DVI-D, Audio, USB2.0, RGB 8.4.1.7. Connections Output: DP Audio 8.4.1.8. External Control: RS232, RJ45, IR Receiver 8.4.1.9. Weight: Should not be more than 25kg 8.4.1.10. Should come with VESA mounting ports 8.4.1.11. Power Consumption not exceeding 160W 8.4.1.12. Certifications: UL/cUL/CB/TUV/KC/, FCC Class "A"/CE/ KCC, Energy Star 6.0 (other related internationally recognized certification scheme)	
	8.5. Video wall Control System 8.5.1. Video wall capabilities should include minimum 8 concurrent displays, PIP, resizing of contents and switching 8.5.2. Matrix switching concept with interactive videowall functionality and KVM 8.5.3. Compose of transceiver boxes that can be as input or output to a display, videowall or to a KVM peripheral 8.5.4. Multi-operator control 8.5.5. Flexible, scalable and Plug and play 8.5.6. Transceivers should be POE based 8.5.7. Videowall capabilities should include minimum 8 concurrent displays, PIP, resizing of contents and switching	
	8.6. Videowall Transceivers (videowall) 8.6.1. Should come with integrated videowall processor, multi-viewer, AV matrix, and extension over CAT5 capability 8.6.2. IP-based configuration 8.6.3. Real time preview of content on the dashboard interface 8.6.4. Direct access for RTSP source/encoder 8.6.5. Full-cross-point audio transmitting and embedding/de-embedding 8.6.6. User rights and permissions can be set	
	8.7. Videowall Transceivers (KVM) 8.7.1. Should be seamless video pull/push to any display or videowall in 1-2 sec 8.7.2. Should be simple plug and play 8.7.3. Should be POE 8.7.4. HDMI+RS232/485_IR/IO_USB over CAT5 transmission 8.7.5. IP based configuration 8.7.6. Direct access for RTSP source/encoder 8.7.7. Should come with cross display switching function: mouse and keyboard can switch across displays 8.7.8. User rights and permissions can be set	
	8.8. Videowall Transceiver Matrix Switch 8.8.1. Provide 48 10/100/1000BASE-T PoE-plus, 4 1000/10GBaseX unpopulated SFP+ ports 8.8.2. Support optional two port 10GBaseX SFP+ or 10GBase-T copper ports modules.	

	8.8.3. Support optional two port 40G QSFP+ ports module. 8.8.4. Support optional G.8232 Synchronous Ethernet (SyncE) and ITU 1588 Precision 8.8.5. Time Protocol (PTP) module. 8.8.6. The switch operating system must be highly resilient and modular. 8.8.7. The switch operating system must allow the installing or upgrading of individual software modules and restart unresponsive process. 8.8.8. Must use same switch operating system image across the proposed access switches models for ease of management. 8.8.9. Allows a single physical switch to be split into multiple VRs. 8.8.10. Provide Multi switch link aggregation group to address bandwidth limitations and improve network resiliency. 8.8.11. Provide 4000 Port-based, Protocol-based, 802.1Q VLANs and 802.1ad VLAN. 8.8.12. Provide RFC3619 Ethernet Automatic Protection Switching with 50 ms recovery. 8.8.13. Provide ITU-T G.8032 Ethernet Ring Protection Switching to enable carrier grade resiliency. 8.8.14. Provide IEEE P802.1Qaz DCBX (Data Center Bridging eXchange) to exchange configuration information with directly connected peers. The protocol can be used for configuring PFC, ETS, and application parameters on peers. The protocol can also be used to detect misconfiguration in peers. 8.8.15. Must provide Kerberos snooping to work with Microsoft Active Directory to track users who access their network. The report should include IP, MAC, VLAN, computer hostname, and port location of the user. 8.8.16. Support following stacking features or provide modular chassis switch: 8.8.16.1. Support up to 8 switches in a stack 8.8.16.2. Support stacking using10GE ports 8.8.16.3. Support at least 40Gbps stacking bandwidth and can scale up to 160Gbps stacking bandwidth 8.8.16.4. Support stacking distance of up to 40km. 8.8.17. Support the ability to authenticate multiple users on a single port via 802.1X, Web or MAC at the same time. 8.8.18. Support dynamic role-based policy, independent of the VLAN assigned to the port, to secure and provision network resources based upon the role the user or device plays within the network.	
	8.9. Smart Board TV (for the SOC Conference Room) 8.9.1. System Specifications 8.9.1.1. Display Panel 8.9.1.1.1. Screen Size: 84” Smart Board TV 8.9.1.1.2. Active Display Area (mm): 1860.48 x 1046.52 8.9.1.1.3. Resolution: 3840 x 2160 (QWUXGA) 8.9.1.1.4. Brightness (cd/m2 typ.): 350 8.9.1.1.5. Response Time (mx, GTG): should not be less than 5 8.9.1.1.6. Life Time (hours): 50,000	

	8.9.1.2. Touch Screen 8.9.1.2.1. Resolution: 32767 x 32767 8.9.1.2.2. Touch Method: Should be pointed including fingers 8.9.1.2.3. Interface: USB 2.0 compatible (full speed), HID compatible, Plug & Play compatible 8.9.1.2.4. Detection Method: Optical Image Sensors 8.9.1.2.5. Operating Systems: Windows XP / Vista / 7 / 8, Linux 2.6X and above, Mac OSX 10.4 and above 8.9.1.2.6. Response Rate: 125 rps or above 8.9.1.3. Connectivity and Control 8.9.1.3.1. Input: DP (1.2), HDMI (2.0), HDMI (1.4), USB 8.9.1.3.2. Output: Speaker (10W x 2CH), Audio (Line out) 8.9.1.4. Feature 8.9.1.4.1. Tempered Glass (mm): 5, Anti-Glare; Auto Brightness Sensor 8.9.1.5. Mechanical (Standard) 8.9.1.5.1. Dimension (mm)/(WxHxL): 2028 x 1214 x 92 8.9.1.5.2. Weight (kg): Should not be greater 100kg 8.9.1.6. Environmental Conditions Operability 8.9.1.6.1. Temperature (°C): 0-40; Humidity (%): 20-80	
	8.10. Two (2) Video Wall Display (For monitoring of the SOC Manager and Assistant Secretary) 8.10.1. Panel Size: 55 ‟ 8.10.2. Aspect Ratio: 16:9 8.10.3. Native Resolution: 1920 x 1080 (FHD) 8.10.4. Brightness: 500 cd/m2 8.10.5. Input 8.10.5.1. Digital: DVI-D, HDMI with HDCP for all input 8.10.5.2. Analog: RGB, AV 8.10.5.3. External Control: RS232C, RJ45, IR Receiver 8.10.5.4. USB: At least USB 2.0 8.10.6. Output 8.10.6.1. Digital: DVI-D 8.10.6.2. External Control:RS232C 8.10.7. Bezel Width: Maximum of 2.25mm (left/top) / 1.25mm (right/bottom) 8.10.8. Temperature Sensor: Yes 8.10.9. Source Selection: Digital (HDMI / DVI) / Analog (RGB) / Component / USB 8.10.10. Operation Temperature: 0°C~40°C 8.10.11. Operation Humidity: Minimum of 10%~80% 8.10.12. Power Supply: 100–240V~, 50/60Hz 8.10.13. Power Consumption: Maximum of 160W 8.10.14. Standard Certification: UL / cUL / CB / TUV / KC / FCC Class "B" / CE / KCC / ENERGY STAR® Qualified (among other related internationally recognized certification scheme)	
	8.11. CCTV Package (8 Indoor and 4 Outdoor) 8.11.1. DVR - 8 Channel AHD DVR	

	8.11.2. DOME CAMERA - 720p AHD Aptina sensor mini eyeball LED array 4x 8.11.3. OUTDOOR - 720p AHD with 10-20m IR Aptina 3.6mm lens 4x 8.11.4. CCTV CABLE - Precut Siamese Cable 8x 8.11.5. POWER SUPPLY -12 Volts 1amp 8x 8.11.6. HARD DISK- 1TB	
	8.12. Access Control Authentication **8.12.1. Finger-Vein Authentication** 8.12.1.1. Application: Access Control 8.12.1.2. Biometric Type: Finger-vein (blood line pattern) 8.12.1.3. Matching Speed: 1 sec or less 8.12.1.4. RF Card Option: 13.56Mhz 8.12.1.5. Capacity Max User : 1,000 8.12.1.6. Max Text Log: 1,000,000 8.12.1.7. Max Image Log: 10,000 8.12.1.8. PoE (Power over Ethernet): Yes 8.12.1.9. Interface TCP/IP: Yes 8.12.1.10. RS-485: 2 Channels 8.12.1.11. RS-232: Yes 8.12.1.12. Wiegand: Yes 8.12.1.13. Relay: 2 Relays 8.12.1.14. USB: Host and Slave 8.12.1.15. Hardware CPU: Cortex-M4 32bit 8.12.1.16. Camera: Built-in Camera for real time image capture 8.12.1.17. LCD Touch Screen: 5.0 inch COLOR TFT LCD 8.12.1.18. Operating Temp.: -20° to +60° 8.12.1.19. Operating Humidity: 10% to 90% 8.12.1.20. Power Supply: 12V, 2.5A 8.12.1.21. Dimensions (mm)/(WxLxH): 162x145x95 8.12.1.22. Weight: 388g 8.12.1.23. Certificate: KCC, CE, FCC, RoHS	
	8.12.2. Keypad Authentication 8.12.2.1. The solution shall provide the following capabilities: 8.12.2.1.1. Integrated photo ID creation capability with video verification. 8.12.2.1.2. User interface secured access under encrypted password control. 8.12.2.1.3. System-wide timed anti-passback function. 8.12.2.1.4. Regional anti-passback with mustering and roll call functions. 8.12.2.1.5. Region occupancy counting and control. 8.12.2.1.6. Dual reader and keypad support. 8.12.2.1.7. "First-in-unlock" rule enforcement. 8.12.2.1.8. Multiple access levels and cards per person. 8.12.2.1.9. 128-bit card support. 8.12.2.1.10. Detailed time specifications. 8.12.2.1.11. Simultaneous support for multiple card data formats. 8.12.2.1.12. Access privileges variable by threat level. 8.12.2.1.13. Schedule portal unlock by time and threat level.	

	8.12.2.1.14. Card format decoder quickly discovers unknown card formats. 8.12.2.1.15. Card enrollment by reader or keyboard. 8.12.2.1.16. Compatibility with various input devices including biometric readers. 8.12.2.1.17. Activation/expiration date/time by person with one minute resolution. 8.12.2.1.18. Merge CSI Spec 3 8.12.2.1.19. Access level disable for immediate lockdown. 8.12.2.1.20. Use of Threat Levels to alter security system behavior globally. 8.12.2.1.21. Multiple holiday schedules. 8.12.2.1.22. Timed unlock schedules. 8.12.2.1.23. Scheduled actions for arming inputs, activating outputs, locking and unlocking portals. 8.12.2.1.24. Card enrollment reader support. 8.12.2.1.25. Counted-use access control. 8.12.2.1.26. Dual-reader portal support. 8.12.2.1.27. Wiegand keypad PIN support. 8.12.2.1.28. 8-bit and 4-bit burst keypad support 8.12.2.1.29. Integration with supported alarm panels. 8.12.2.1.30. Optional storage and recall of ID photos and personal/emergency data. 8.12.2.1.31. The solution shall provide the following Alarm Monitoring capabilities: 8.12.2.1.32. Common alarm panel integration for disarm on access, and arm on egress. 8.12.2.1.33. Integrated alarm monitoring and event management with alarm panels. 8.12.2.1.34. Provide alarms on video loss, and video motion detection. 8.12.2.1.35. Provide for alarms on communication loss and temperature variation. 8.12.2.1.36. Support the creation of custom sets of alarm event actions. 8.12.2.1.37. Provide the ability to record video for alarm events. 8.12.2.1.38. Provide the ability to assign threat levels to various alarms according to severity. 8.12.2.1.39. Provide system generated email or text message alerts. 8.12.2.1.40. Support electronic supervision of alarm inputs. 8.12.2.1.41. Support the use of output relays for enabling circuits under alarm event control. 8.12.2.1.42. A monitoring desktop that integrates video, system activity logs, floor plans, ID photos, and alarm notifications. 8.12.2.1.43. Graphic floor plans with active icons of security system resources. 8.12.2.1.44. System user permissions to grant whole or partial access to system resources, commands, and personal data. 8.12.2.1.45. Delivery of alerts via browsers, email, and text messages.	

	8.12.2.1.46. The system shall provide the following Video Management capabilities: 8.12.2.1.47. Real-time video monitoring displays, including multiple cameras simultaneously. 8.12.2.1.48. Playback of access-related video. 8.12.2.1.49. Video switching based on access activity or event activation. 8.12.2.1.50. Integrated alarm inputs from the video management system. 8.12.2.1.51. Digital recording of events. 8.12.2.1.52. Support for multiple DVR and NVR systems. 8.12.2.1.53. Multiple supported cameras. 8.12.2.1.54. Recall of photo ID and real-time image for comparison. 8.12.2.1.55. Full monitoring through a web browser interface. 8.12.2.1.56. System user permissions to grant whole or partial access to system cameras and video resources. 8.12.2.1.57. The solution shall provide the following Security Database capabilities: 8.12.2.1.58. Maintain data of system activity, personnel access control information, system user passwords and custom user role permissions for whole or partial access to system resources and data. 8.12.2.1.59. Built-in Open Database Connectivity (ODBC) compliant database for personal data. 8.12.2.1.60. Up to 60,000 person records. 8.12.2.1.61. Network-secure API for external application integration. 8.12.2.1.62. Extensive and easy to use custom report generator. 8.12.2.1.63. User-defined data fields in personnel records. 8.12.2.1.64. Record recall by vehicle tag, name, or card. 8.12.2.1.65. SQL capability and ODBC compliance. 8.12.2.1.66. Storage of system user passwords and permissions. 8.12.2.1.67. Storage and recall of ID photos and emergency personal information. 8.12.2.1.68. Pre-defined reports on system configuration, system activity history, and people. 8.12.2.1.69. English-based query language for instant custom reports. 8.12.2.1.70. Custom report writer interface that allows the interactive creation of custom reports. Reports may be saved for later reuse. No third party software (such as Crystal Reports) shall be necessary. 8.12.2.1.71. Periodic backup to onboard flash ROM and optional network attached storage (NAS), including FTP servers. 8.12.2.1.72. Email and text messaging (SMS) text messaging alert notification	
	8.13. SOC Desktop Package (9 units) 8.13.1. **Technical Specifications** 8.13.1.1. Swift Curved Monitor – 34” 21:9 Ultra-wide QHD (3440×1440), overclockable 100Hz , G-SYNC™	

	8.13.1.2. Intel Core i9-7920X with motherboard 8.13.1.3. At least 32GB RAM Memory 8.13.1.4. Minimum 8GIG VIDEO card dedicated 8.13.1.5. 480GB SSD + 2TB HDD 8.13.1.6. Integrated Ethernet plugs into your compatible wired network 8.13.1.7. USB 3.0 ports 8.13.1.8. Windows 10 Pro latest edition 8.13.1.9. include high-end keyboard / mouse	
9.	**Training / Knowledge Transfer / Capacity Building**	
	8.14. The Vendor shall provide certification operational training to the SOC Manager, Analysts, and relevant technical staff on the SOC system as part of the project implementation process. 8.15. The SOC Operational Training agenda shall include, but not limited to: 8.15.1. The cyber domain threat actors attack vectors 8.15.2. Solution capabilities and architecture 8.15.3. Solution GUI 8.15.4. Using detection engines and forensics tools 8.15.5. Conducting investigation workflow by simulating real attack scenarios 8.15.6. Using the SOC platform's web-tools for investigation enrichment 8.15.7. Methodology and workflow 8.15.8. Intelligence feeds updates and using management tools 8.16. The Vendor shall provide maintenance training to the Support Engineers, and System Administrators as part of the project implementation process. 8.16.1. The SOC Maintenance Training agenda shall include: 8.16.1.1. System architecture 8.16.1.2. System flows 8.16.1.3. Frontend subsystem overview 8.16.1.4. Backend subsystem overview 8.16.1.5. Maintenance tools overview 8.17. The Vendor shall provide operational training to the Analysts on the operation of the DarkWeb investigation tools as part of the project implementation process. 8.18. Knowledge Transfer – prior to the issuance of Certificate of Final Acceptance, the winning vendor must conduct a thorough solution walk through for DICT nominated personnel. The intent primarily is to orient these personnel on the completed installations, equipment type, functionalities, configurations and how the newly installed security systems augment the existing security infrastructure. The knowledge Transfer must cover the following, but not limited to: 8.18.1. Equipment Technical Specifications i.e. functional features and other relevant technical data. 8.18.2. Basic Appliance and Software Operations i.e. menu navigation, basic reconfiguration, and other relevant information pertaining to normal operations of the equipment. 8.18.3. Troubleshooting - SI must provide sample occurrences and step by step procedures in addressing technical issues allowed by the equipment	

manufacturer to be carried out by the end-user without voiding active warranty.

8.18.4. Preventive Maintenance Orientation - contractor must conduct a detailed walk-through of the processes and/or procedures to be performed during Maintenances Services.

8.18.5. Support Service Structure - SI must present the applicable Support Structure, Support Escalation Levels and valid contact details.

All areas covered during the Knowledge Transfer sessions should be accurately documented and compiled in the Operations & Maintenance manual which forms part of the SI's submittals.

8.19. At a minimum, the Knowledge Transfer session must include the following:

8.19.1. Classroom session - presentation of designs, equipment specifications, equipment functionality, back-up systems, troubleshooting, operations and maintenance.

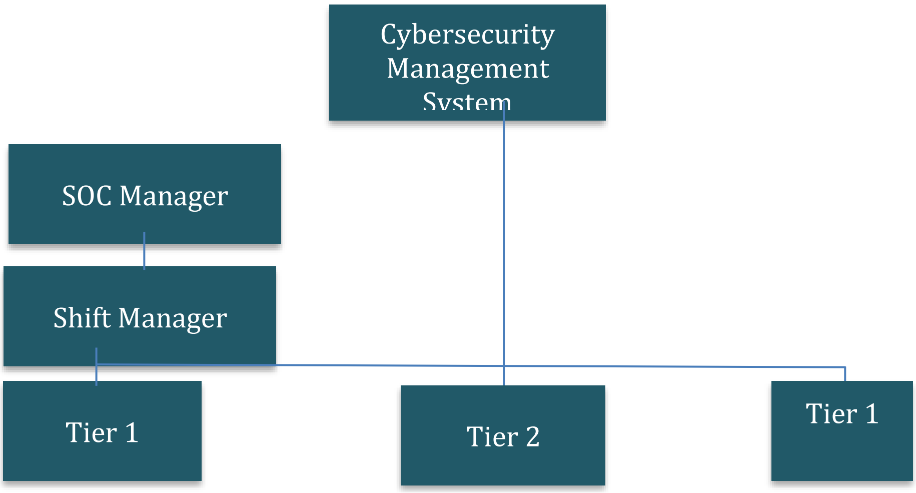
8.19.2. Solutions Walk-Through - physical inspection of all installed equipment and devices, operation demonstration i.e. power up/down, settings, basic configuration, etc.

9. **Operation**

10.1. The vendor shall make sure that all access to Analyst computers shall be two-factor authenticated i.e. Bio Authenticated – Face and Finger-Vein Authentication.

9.1.1. The Vendor shall assist DICT in staffing the CMS team in three years up to a complete transfer of knowledge is achieved. This shall include at least one (1) personnel on each tier from Tier-1 to Tier-3 and another one (1) personnel that will act as a Supervisor.

CMS Organizational Structure: (Internal) – *The CMS will work on a three (3) shift operation.*



	9.1.2. The Vendor shall provide analysts and consultants based on the following criteria: 9.1.2.1. The analyst shall be a Filipino citizen 9.1.2.2. The consultant may either be a Filipino or any citizenship. 9.1.2.3. The analyst must be a holder of at least any internationally recognized relevant security certification and has a minimum solid experience of two (2) years in the field of cybersecurity. 9.1.2.4. The Vendor shall see to it that the SOC Manager shall be able to perform at least the following: 9.1.2.4.1. Assign incidents to analysts 9.1.2.4.2. Manage and monitor the performance of SOC team members 9.1.2.4.3. Track incident handling by KPIs (using the dashboard), threat types, and levels 9.1.2.4.4. Monitor all tasks performed by the analyst / senior analyst 9.1.2.5. The vendor shall see to it that the SOC Analyst / Senior analyst shall be able to perform at least the following: 9.1.2.5.1. Review assigned incidents by severity. 9.1.2.5.2. Investigate the incident using the following tools: 9.1.2.5.2.1. Network Forensics 9.1.2.5.2.2. Endpoint Forensics 9.1.2.5.2.3. File Analysis 9.1.2.5.2.4. Online Web search 9.1.2.5.2.5. Search Alerts 9.1.2.5.2.6. Search Incidents 9.1.2.5.3. Add evidence and observations to the incident findings and workflow. 9.1.2.5.4. Respond to incidents as follows: 9.1.2.5.4.1. Mark as actionable intelligence. 9.1.2.5.4.2. Manually create rules based on investigation outcome. 9.1.2.5.4.3. Escalate to a higher level analyst or SOC manager/CISO (if required) by changing the incident status. 9.1.2.5.5. Update incident status/severity. 9.1.2.5.6. Launch proactive investigations using the solution's investigation tools (typically by senior analysts). 9.1.2.5.7. Open new incidents based on evidence and investigation findings. 9.1.2.5.8. Set alert action rules to optimize the investigation process and reflect priorities (Intelligence module).	
10.	**Warranty** 10.1. The vendor shall replace defective items to the end-user within fifteen (15) calendar days from receipt of Notice of Defects from DICT. Service units from the vendor shall be provided while waiting for replacement.	

	10.2. Warranty issued in each component in the core shall be valid for twenty-four (24) months. Components shall include all equipment in the CMS: Tools, servers, and other physical parameters such as but not limited to computers, video wall display, and authentication devices.	
11.	**Escalation** 11.1. The vendor shall provide technical support or assistance to the end-user in case of emergency and/or failure to the hardware/software in the CMSP's network. 11.2. The vendor shall provide the following support to the CMS: 11.2.1. Hardware / Software Support. 11.2.1.1. Replacement of the hardware and software support will be base on the Warranty and Support acquisition entitlement of the equipment. 11.2.2. Scope of Responsibility – The scope of work covers the following: 11.2.2.1. Troubleshooting and configuration on-site. 11.2.2.2. Replace defective equipment and configure it. 11.2.2.3. Update firmware as necessary.	
12.	**Licenses and Support** 12.1. All software in the above mentioned shall have three (3) years perpetual license from the vendor. The end-user is entitled to download all updates to the software and receive technical support from the vendor. After the period ends, the end-user has the privilege to remain with the last version downloaded or to purchase a 1 year Updates & Support package, for 20% of the license price. 12.2. Support and maintenance to the core and deployed tools in the priority agencies shall be valid for three (3) years.	
13.	**Compatibility and Interoperability with Open System Platform** All supplied equipment, devices and/or systems must not proprietary and are capable of integration with a third (3rd) party open system monitoring platform. Brand lock-in is not acceptable.	
14.	**Penalty Clause** Winning vendor is mandated by DICT to deliver its proposed services within the mutually agreed Work Plan. In the event that the contractor is not able to deliver within the allowable and acceptable period, DICT shall impose a Delay Penalty of one tenth (1/10) of one (1) percent of the cost of the unperformed portion for every day of delay until actual delivery or performance. Penalty shall be imposed if final acceptance date is not achieved as per agreed Project Work Plan. Should the delay/s is/are due to unavoidable circumstances i.e. typhoon, earthquakes or other natural disasters, delays caused by the Project (DICT) and other forms of delays not within the control of the winning bidder, the winning bidder must provide a written report detailing the cause of delay, impacted deliverables with reasons thereof and a detailed catch up plan and/or updated work plan. This must then be presented to DICT's project team for discussion and acceptance.	

15. **Payment Terms / Progress Payment**

The Payment Terms for this project shall be Milestone based per defined deliverables, validation by DICT Project Manager and Sign-Off. Payment milestones are tabulated below:

Milestones	Progress
Upon onsite delivery of all Hardware/Software	10%
Upon completion of installation and configurations	10%
Upon completion of agreed Testing	10%
Upon execution of VAPT to the Cybersecurity Management System's Network	5%
Completion of Testing to the Cybersecurity Management System's Network	20%
Upon Installation and Configuration of Hardware/Software to the Priority Agencies	10%
Upon completion of operational stress test to the Cybersecurity Management System and Priority Agencies Network	15%
Upon completion of Knowledge Transfers and submission of As – Built Plans, Operations & Maintenance Manuals, Warranty completion of Training Sessions	20%
Total	**100%**

16. **Timelines for Implementation of the Project**

As stated in this document, the projected implementation duration is maximum of 10 months from date of award. Vendor proposed implementation schedule must not exceed 10 months. Such projections are based on the following Work Breakdown

Description	Duration
Hardware/Software Onsite Delivery	1 Month
Installation and configuration	0.5 Month
Testing and Submission of Testing Results & Documentations	0.5 Month
CMS Network VAPT	0.5 Month
Hardware/Software Delivery to Priority Agencies	2 Month
Installation and Configuration of Hardware/Software to Priority Agencies	2 Month
Operational Stress Test	0.5 Month
Knowledge Transfer	3 Months
Total	**10 Months**

Structure (WBS):

17. **Service Level Agreement**

Agreement between the Contractor and DICT that defines the Service Levels, terms and conditions for enforcing the Service Levels and the remedies in case the service levels are not fulfilled.

Security Level	**Maximum Response Time** (from the time problem is determined during the response time to the time of resolution)
High/Critical/Down	Four (4) Hours
Medium/Normal	Next Day
Low/General Question	Two (2) Business Days

Name of Company

Signature Over Printed Name
Of Authorized Representative

Date

Section VIII.
Bidding Forms

Annex I

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

STATEMENT OF ALL ONGOING GOVERNMENT AND PRIVATE CONTRACTS

All On-Going Contracts (including contract/s awarded but not yet started, if any)

Name of Client	Name of the Contract	Date and Status of the Contract	Kinds of Goods	Amount of Contract	Value of Outstanding Contracts	Date of Delivery	Purchase Order Number/s or Date of Contract/s

Name & Signature of Authorized Representative

Position

Date

Instructions:

1. State all on-going contracts including those awarded but not yet started (Government and Private Contracts which may be similar or not similar to the project called for bidding as of the **day before the deadline** of submission of bids.
2. If there is **NO** on-going contract including awarded but not yet started as of the abovementioned period, state none or equivalent term.
3. The total amount of the ongoing but not yet started contracts should be consistent with those used in the Financial Contracting Capacity (NFCC).

Annex I-A

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

STATEMENT OF SINGLE (1) LARGEST COMPLETED CONTRACT OF SIMILAR NATURE WITHIN THE LAST FIVE (5) YEARS FROM DATE OF SUBMISSION AND RECEIPT OF BIDS AMOUNTING TO AT LEAST FIFTY PERCENT (50%) OF THE APPROVED BUDGET FOR THE CONTRACT (ABC)

Name of Client	Name of Contract	Date of the Contract	Kinds of Goods	Value of Contracts	Date of Completion	Official Receipt No. & Date OR End User's Acceptance Date

CERTIFIED CORRECT:

____
Name & Signature of Authorized Representative

____
Position

____
Date

Instructions:

1. Cut Off Date as of: (i) Up to the day before the deadline of submission of bids.
2. In the column under "Dates", indicate the dates of Delivery/End-User's Acceptance and Official Receipt No.
3. Name of Contract column, indicates the Nature/Scope of the Contract for the DICT to determine the relevance of the entry with the Procurement at hand.

Annex II

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

CERTIFICATE OF NET FINANCIAL CONTRACTING CAPACITY
(Please show figures at how you arrived at the NFCC)

This is to certify that our **Net Financial Contracting Capacity (NFCC)** is **Philippine Pesos ______________ (₱________________)** which is at least equal to the Approved Budget for the Contract (ABC). The amount is computed as follows:

> NFCC = [{Current Assets minus Current Liabilities) (15)] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started coinciding with the contract to be bid.
>
> NFCC = (CA-CL) (15) – C

Issued this _____ day of __________, 2018.

CERTIFIED CORRECT:

____
Name & Signature of Authorized Representative

____
Position

____
Date

Notes:

1. The values of the bidder’s current assets and current liabilities be based on the data submitted to BIR through its Electronic Filing and Payment System.
2. Value of all outstanding or uncompleted contracts refers those listed in Annex-I.
3. The detailed computation using the required formula must be shown as provided above.
4. The NFCC computation must at least be equal to the total ABC of the project**.**

Annex III
(page 1 of 3)

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT BAC4G&S-2018-002

PROTOCOL / UNDERTAKING OF AGREEMENT TO ENTER INTO JOINT VENTURE

This **PROTOCOL / UNDERTAKING OF AGREEMENT TO ENTER INTO JOINT VENTURE,** executed by:

__________ a sole proprietorship/partnership/corporation duly organized and existing under and by virtue of the laws of the Philippines, with offices located at __________, __________, representative herein by __________, __________, hereinafter referred to as "__________";
-and-
__________ a sole proprietorship/partnership/corporation duly organized and existing under and by virtue of the laws of the Philippines, with offices located at __________, __________, representative herein by __________, __________, hereinafter referred to as "__________";
-and-
__________ a sole proprietorship/partnership/corporation duly organized and existing under and by virtue of the laws of the Philippines, with offices located at __________, __________, representative herein by __________, __________, hereinafter referred to as "__________";
(hereinafter referred to collectively as "Parties")

For submission to the **Bids and Awards Committee** of the **Department of Information and Communications Technology**, pursuant to **Section 23.1 (b)** of the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (R.A.) 9184.

WITNESSETH That:

WHEREAS, the Parties desire to participate as a Joint Venture in the public bidding that will be conducted by the **Department of Information and Communications Technology**, pursuant Republic Act (R.A.) 9184 and its Implementing Rules and Regulations, with the following particulars:

Bid Reference No.	**BAC4G&S-2018-002**
Name/Title of Procurement Project	**SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT**
Approved Budget for the Contract	**PhP512,000,000.00**

Annex III
(page 2 of 3)

NOW THEREFORE, in consideration of the foregoing, the Parties undertake to enter into a **JOINT VENTURE** and sign a **Joint Venture Agreement** relative to the joint cooperation for this bid project, in the event that their bid successful, furnishing the copy thereof within **ten (10) calendar days** from receipt of Notice from the BAC that our bid has the lowest calculated bid or highest rated responsive bid (as the case may be).

For the purposes of this bid project, and unless modified by the terms of the Joint Venture Agreement, the following party shall be the authorized representative of the JV:

CERTIFIED CORRECT:

______________________	______________________
Authorized Representative of the JV Partner: (Per attached Secretary's Certificate)	Authorized Representative of the JV Partner: (Per attached Secretary's Certificate)
______________________	______________________
Name	Name
______________________	______________________
Date	Date

Furthermore, the parties agree to be bound jointly and severally under the said Joint Venture Agreement;

THAT Finally, failure on our part of enter into the Joint Venture and/or sign the Joint Venture Agreement for any reason after the Notice of Award has been issued by shall be a ground for non-issuance by DICT of the Notice to Proceed, forfeiture of our bid security and such other administrative and/or civil liabilities as may be imposed by DICT under the provisions of R.A. 9184 and its 2016Revised IRR, without any liability on the part of DICT.

This Undertaking shall form an integral part of our Eligibility documents for the above-cited project.

IN WITNESS WHEREOF, the parties have singed this Protocol/Undertaking on the date fist above-written.

Bidder's Representative/Authorized Signature

[JURAT]

SUBSCRIBED AND SWORN TO BEFORE ME this __________ day of __________ at __________, Philippines, affiant exhibited to me his/her competent Evidence of Identity (as defined by 2004 Rules on Notarial Practice issued at _________ at __________, Philippines.

Doc No. _______
Page No. ______
Book No. ______
Series of ______

Annex III

(page 3 of 3)

Note:
"Sec.12. Competent Evidence of Identity - The phrase” competent evidence of identity" refers to the identification of an individual based on:
At least one current identification documents issued by an official agency bearing the photograph and signature of the individual, such as but limited to, passport, driver's license, Professional Regulations Commission ID, National Bureau of Investigation clearance, police clearance, postal ID, voter's ID, Barangay Certification, Government Service and Insurance System (GSIS) e-card, Social Security System (SSS) card, PhilHealth card, senior citizen card, Overseas Workers Welfare Administration (OWWA) ID, OFW ID, seaman's book, alien certificate of registration/immigrant certificate of registration, government office ID, certification from the National Council for the Welfare of Disabled Persons (NCWDP), Department of Social Welfare and Development (DSWD) certification.

Annex IV
(page 1 of 2)

REPUBLIC OF THE PHILIPPINES)
CITY OF _________________________) S.S.

BID-SECURING DECLARATION

Invitation to Bid Reference No.: BAC4G&S-2018-002

To: *[Insert name and address of the Procuring Entity]*

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid-Securing Declaration.

2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, if I/we have committed any of the following actions:

   (i) Withdrawn my/our Bid during the period of bid validity required in the Bidding Documents; or

   (ii) Fail or refuse to accept the award and enter into contract or perform any and all acts necessary to the execution of the Contract, in accordance with the Bidding Documents after having been notified of your acceptance of our Bid during the period of bid validity.

3. I/We understand that this Bid-Securing Declaration shall cease to be valid on the following circumstances:

   (a) Upon expiration of the bid validity period, or any extension thereof pursuant to your request;

   (b) I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right;

   (c) I am/we are declared as the bidder with the Single/Lowest Calculated and Responsive Bid/Highest Rated and Responsive Bid, and I/we have furnished the performance security and signed the Contract.

Annex IV
(page 2 of 2)

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this ____ day of [month] [year] at [place of execution].

[Insert NAME OF BIDDER'S AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

SUBSCRIBED AND SWORN to [place of execution], Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her [insert type of government identification card used], with his/her photograph and signature appearing thereon, with no. ______ and his/her Community Tax Certificate No. _______ issued on ______ at ______.

Witness my hand and seal this ___ day of [month] [year].

NAME OF NOTARY PUBLIC
Serial No. of Commission ___________
Notary Public for ______ until _______
Roll of Attorneys No. _____
PTR No. __, [date issued], [place Issued]
IBP No. __, [date issued], [place issued]

Doc. No. ___
Page No. ___
Book No. ___
Series of ____.

Note:
"Sec.12. Competent Evidence of Identity - The phrase" competent evidence of identity" refers to the identification of an individual based on:
At least one current identification documents issued by an official agency bearing the photograph and signature of the individual, such as but limited to, passport, driver's license, Professional Regulations Commission ID, National Bureau of Investigation clearance, police clearance, postal ID, voter's ID, Barangay Certification, Government Service and Insurance System (GSIS) e-card, Social Security System (SSS) card, PhilHealth card, senior citizen card, Overseas Workers Welfare Administration (OWWA) ID, OFW ID, seaman's book, alien certificate of registration/immigrant certificate of registration, government office ID, certification from the National Council for the Welfare of Disabled Persons (NCWDP), Department of Social Welfare and Development (DSWD) certification.

Annex V

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

OMNIBUS SWORN STATEMENT

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _______) S.S.

AFFIDAVIT

I/We, _____________, of legal age, with residence at ___________, after having duly sworn in accordance with law and in compliance with the bidding requirements as contained in the Instructions to Bidders/Bid Data Sheet for the bidding do hereby certify under oath as follows:

(a)
AUTHORITY OF THE DESIGNATED REPRESENTATVE

(Please check appropriate box and full up blanks)

□ **LE PROPRIETORSHIP**

That I am the sole proprietor of <Company Name/Name of Supplier> with business address at _____________; Telephone No. ________________, with Fax No. __________ and e-mail address ______________ and as such, I have the full power and authority to do, execute, and perform any and all acts necessary to represent it in the negotiation.

Name:____________________________
Title:_____________________________
Specimen Signature:_________________

OR

That I am the <Company Name/Name of Supplier> with business address at _____________; Telephone No. ________________, with Fax No. __________ and e-mail address ______________ and as such, I have the full power and authority to do, execute, and perform any and all acts necessary to represent it in the negotiation.

Name:____________________________
Title:_____________________________
Specimen Signature:_________________

Note: Please attach a Special Power of Attorney, if not the Sole Proprietor/Owner.

□ **RPORATION, PARTNERSHIP, COOPERATIVE**

That I/We am/are the duly authorized representative/s of <Company Name>, located at _____________; Telephone No. ________________, with Fax No. __________ and e-mail address ______________; as shown in the attached Secretary's Certificate issued by the corporation or the members of the joint venture, and granted full power and authority to execute and perform any and all acts necessary and/or to represent our company in the abovementioned negotiations, including signing all negotiation documents and other related documents such as the contracts:

1. Name:____________________________
   Title:____________________________
   Specimen Signature:_________________
2. Name:____________________________
   Title:____________________________
   Specimen Signature:_________________

Note: Please attach duly executed Secretary's Certificate.

(b)
NON-INCLUSION IN THE BLACKLIST NOR UNDER SUSPENSION STATUS BY ANY AGENCY OR GOVERNMENT INSTRUMENTALITY

That the firm I/We represent is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, Foreign Government/Foreign or International Institution whose blacklisting rules been recognized by the Government Procuring Policy Board;

(c)
AUTHENTICITY OF SUBMITTED DOCUMENTS

That each of the documents submitted by our company by our company in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct.

(d)
AUTHORITY TO VALIDATE SUBMITTED DOCUMENTS

The undersigned duly authorized representative of the Applicant, for and in behalf of the Applicant hereby submits this Letter of Authorization in relation with Application to apply for Eligibility and to Bid for the subject contract to be bid.

In the connection thereat, all public official, engineer, architect, surety company, bank institution or other person, company or corporation named in the eligibility documents and statements are hereby requested and authorized to furnish the Chairperson of Bids and Awards Committee or his duly authorized representative/s any information necessary to verify the correctness and authenticity of any item stated in the said document and statements or regarding our competence and general reputation.

I/We hereby give consent and give authority to the Chairperson of Bids and Awards Committee or his duly authorized representative, to verify the authenticity and correctness, of any or all of the documents and statements submitted herein; and that I/we hereby hold myself liable, criminally or civilly, for any misrepresentation or false statements made therein which shall be ground for outright disqualification and/or ineligibility, and inclusion of my/our company among the contractors blacklisted from participating in future biddings of **Department of Information and Communications Technology .**

(e)
DISCLOSURE OF RELATIONS

That for and in behalf of the Bidder, I/We hereby declare that:

□ e bidder is an individual or a sole proprietorship, to the bidder himself;
□ e bidder is a partnership or cooperative, to all its officers and members;
□ e bidder is a corporation or joint venture, to all its officers, directors, and controlling stockholders;

Are not related by consanguinity or affinity up to the third civil degree with the **Secretary, Officers or Employees** having direct access to information that may substantially affect the result of the bidding such as, but not limited to, **the members of the BAC, the members of the Technical Working Group (TWG), the BAC Secretariat, and DICT.** It is fully understood that the existence of the aforesaid relation by consanguinity or affinity of the Bidder with the aforementioned Officers of the Agency shall automatically disqualify the Bid.

(f) COMPLIANCE WITH EXISTING LABOR LAWS AND STANDARDS

That our company diligently abides and complies with existing labor laws and standards

(g) BIDDER'S RESPONSIBLITIES

1. That I/we have taken steps to carefully examine all of the Bidding Documents;
2. That I/We acknowledge all conditions, local or otherwise, affecting the implementation of the Contract;
3. That I/We made an estimate of the facilities available and needed for the contract to be bid, if any;
4. That I/We will inquire or secure Supplemental/Bid Bulletin(s) issued for this Project.
5. That the submission of all bidding requirements shall be regarded as acceptance of all conditions of bidding and all requirements of authorities responsible for certifying compliance of the contract;
6. That I have complied with our responsibility as provided for in the bidding documents and all Supplemental / Bid Bulletins;
7. That failure to observe any of the above responsibilities shall be at my own risk; and
8. That I agree to be bound by the terms and conditions stated in the Conditions of the Contract for this project.

(h) DID NOT PAY ANY FORM OF CONSIDERATION

That our company did not give or pay directly or indirectly any commission, amount, fee or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

(i) COMPANY OFFICIAL CONTACT REFERENCE

That our company hereby assigns the following contact number/s and e-mail address/es as the official telephone/fax number and contact reference of the company where the DICT Bids and Awards Committee notices be transmitted.

Telephone No./s: ____________________________
Fax No/s. : ________________________________
E-mail Add/s.:______________________________

It is understood that notice/s transmitted in the above-stated telephone/fax numbers and/or e-mail address/es are deemed received as of its transmittal and the reckoning period for the reglementary periods stated in the bidding documents and the revised Implementing Rules and Regulations of Republic Act No. 9184 shall commence from receipt thereof.

IN WITNESS WHEREOF, I have hereunto set my hand this __ day of ___, 20__ at ____________, Philippines.

____
Bidder's Representative/Authorized Signatory

[JURAT]

SUBSCRIBED AND SWORN TO BEFORE ME this _________ day of ________________ at __________________, Philippines. Affiant exhibited to me his/her competent Evidence of Identity (as defined by the 2004 Rules of Notarial Practice ________________ issued ______________ at ____________________, Philippines.

Doc. No._______
Page No._______
Book No._______
Series of_______

Note:
"Sec.12. Competent Evidence of Identity - The phrase" competent evidence of identity" refers to the identification of an individual based on:
At least one current identification documents issued by an official agency bearing the photograph and signature of the individual, such as but limited to, passport, driver's license, Professional Regulations Commission ID, National Bureau of Investigation clearance, police clearance, postal ID, voter's ID, Barangay Certification, Government Service and Insurance System (GSIS) e-card, Social Security System (SSS) card, PhilHealth card, senior citizen card, Overseas Workers Welfare Administration (OWWA) ID, OFW ID, seaman's book, alien certificate of registration/immigrant certificate of registration, government office ID, certification from the National Council for the Welfare of Disabled Persons (NCWDP), Department of Social Welfare and Development (DSWD) certification.

Annex VI

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

COMPANY PROFILE

COMPANY NAME	:
ADDRESS	:
HEAD OFFICE	:
BRANCH	:
TELEPHONE NUMBER/S	:
HEAD OFFICE	:
BRANCH	:
FAX NUMBER/S	:
HEAD OFFICE	:
BRANCH	:
E-MAIL ADDRESS/ES	:
NUMBER OF YEARS IN BUSINESS	:
NUMBER OF EMPLOYEES	:
LIST OF MAJOR STOCKHOLDERS	:
LIST OF BOARD DIRECTORS	:
LIST OF KEY PERSONNEL (NAME & DESIGNATION WITH SIGNATURE) AS AUTHORIZED CONTACT PERSONS FOR THIS PROJECT [at least THREE (3)]	:

____
Name & Signature of Company Authorized Representative

____
Position

____
Date

REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

Annex VII

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

CERTIFICATE OF PERFORMANCE EVALUATION

[Rating of at least Satisfactory to be issued by the Bidder's Single Largest Completed Contract Client indicated in the submitted Annex I-A on the performance of the product supplied / delivered by the prospective bidder]

This is to certify that ___(NAME OF BIDDER)___has supplied our company/agency with __(Name of Product/s)__. Based on our evaluation on timely delivery, compliance to specifications and performance, warranty and after sales service, we give __(NAME OF BIDDER)__ a rating of:

□ VERY SATISFACTORY
□ SATISFACTORY
□ POOR

This Certification shall form part of the Technical Documentary Requirements in line with __(Name of Bidder)__participation in the **SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT** for the Department of Information and Communications Technology .

Issued this _________ day of ___________ 2018 in ____________, Philippines.

Name of Company (Bidder's Client)	Full name of Authorized Representative
Address	Signature of Authorized Representative
Tel. No. / Fax	E-Mail Address

Annex VIII
(page 1 of 4)

PLEASE USE THIS BID FORM. DO NOT RETYPE OR ALTER.

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

TECHNICAL BID FORM

INSTRUCTION TO THE SUPPLIER: Indicate **"COMPLY"** (per line number) under **Bidder's Statement of Compliance** if Bidder can meet the technical specifications and project requirements. DO NOT LEAVE ANY BLANK. A "YES" or "NO" ENTRY WILL NOT BE ACCEPTED. FAILURE TO CONFORM WILL RESULT IN A RATING OF "FAILED".

Line No.:	Project Requirements	Bidder's Statement of Compliance
1	**DICT's Section VII Technical Specifications** For the **SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT**	

Line No.:	ITEM	BRAND	MODEL
2	a. Cyber Intelligence Platform		
	b. Network Protection Tools		
	c. Monitoring Tools		
	d. Log Collection and Correlation		
	e. Management Tools		
	f. Artificial Intelligence / Machine Learning		
	h. Portable CMS		

BIDDER'S UNDERTAKING

I/We, the undersigned bidder, having examined the Bidding Documents including Bid Bulletins, as applicable hereby OFFER to (supply/deliver/perform) the above described items.

I/We undertake, if our bid is accepted, to deliver the items in accordance with the terms and conditions contained in the bid documents, including the posting of the required performance security **within ten (10) calendar days** from receipt of the Notice of Award.

Until a formal contract/order confirmation is prepared and signed, this Bid is binding on us.

Name of Company (in print)

Signature of Company Authorized Representative

Name and Designation (in print)

Date

Annex VIII
(page 2 of 4)

PLEASE USE THIS BID FORM. DO NOT RETYPE OR ALTER.

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT BAC4G&S-2018-002

TECHNICAL BID FORM

INSTRUCTION TO THE SUPPLIER: Indicate **"COMPLY"** (per line number) under **Bidder's Statement of Compliance** if Bidder can meet the technical specifications and project requirements. DO NOT LEAVE ANY BLANK. A "YES" or "NO" ENTRY WILL NOT BE ACCEPTED. FAILURE TO CONFORM WILL RESULT IN A RATING OF "FAILED".

Line No.:	Project Requirements		Bidder's Statement of Compliance
	ITEM	**BRAND**	**MODEL**
2	i. Disaster Recovery Management System		
	j. Storage		
	k. VAPT Tools		
	l. Training and Services		
	m. Network Infrastructure		
	n. Other SOC Equipment and Civil Works		

BIDDER'S UNDERTAKING

I/We, the undersigned bidder, having examined the Bidding Documents including Bid Bulletins, as applicable hereby OFFER to (supply/deliver/perform) the above described items.

I/We undertake, if our bid is accepted, to deliver the items in accordance with the terms and conditions contained in the bid documents, including the posting of the required performance security **within ten (10) calendar days** from receipt of the Notice of Award.

Until a formal contract/order confirmation is prepared and signed, this Bid is binding on us.

Name of Company (in print)

Signature of Company Authorized Representative

Name and Designation (in print)

Date

Annex VIII
(page 3 of 4)

PLEASE USE THIS BID FORM. DO NOT RETYPE OR ALTER.

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

TECHNICAL BID FORM

INSTRUCTION TO THE SUPPLIER: Indicate **"COMPLY"** (per line number) under **Bidder's Statement of Compliance** if Bidder can meet the technical specifications and project requirements. DO NOT LEAVE ANY BLANK. A "YES" or "NO" ENTRY WILL NOT BE ACCEPTED. FAILURE TO CONFORM WILL RESULT IN A RATING OF "FAILED".

Line No.:	Other Requirements	Bidder's Statement of Compliance
3	Bidder has no overdue deliveries or unperformed services intended for the DICT	
4	Bidder did not participate as consultant in the preparation of the design or technical specifications of the GOODS as subject of the bid	
5	**Delivery Place and Distribution** 49 Don A. Roces Ave, Diliman, Quezon City	
6	**Delivery Period** Ten (10) months from receipt of Notice to Proceed	

BIDDER'S UNDERTAKING

I/We, the undersigned bidder, having examined the Bidding Documents including Bid Bulletins, as applicable hereby OFFER to (supply/deliver/perform) the above described items.

I/We undertake, if our bid is accepted, to deliver the items in accordance with the terms and conditions contained in the bid documents, including the posting of the required performance security **within ten (10) calendar days** from receipt of the Notice of Award.

Until a formal contract/order confirmation is prepared and signed, this Bid is binding on us.

Name of Company (in print)

Signature of Company Authorized Representative

Name and Designation (in print)

Date

Annex VIII
(page 4 of 4)

PLEASE USE THIS BID FORM. DO NOT RETYPE OR ALTER.

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

TECHNICAL BID FORM

INSTRUCTION TO THE SUPPLIER: Indicate **"COMPLY"** (per line number) under **Bidder's Statement of Compliance** if Bidder can meet the technical specifications and project requirements. DO NOT LEAVE ANY BLANK. A "YES" or "NO" ENTRY WILL NOT BE ACCEPTED. FAILURE TO CONFORM WILL RESULT IN A RATING OF "FAILED".

Line No.:	Project Requirements If Awarded the Contract		Bidder's Statement of Compliance
7	**Operations and Maintenance Manual**	To submit Operation and Maintenance Manual upon completion of the project (in CD and hard copy).	
8	**Replacement of Defective Items**	Replacement of defective items delivered within fifteen (15) calendar days from receipt of Notice of Defects from DICT. Service unit must be provided while awaiting replacement.	
9	**Warranty**	Warranty Certificate issued for two (2) years in favor of DICT.	

BIDDER'S UNDERTAKING

I/We, the undersigned bidder, having examined the Bidding Documents including Bid Bulletins, as applicable hereby OFFER to (supply/deliver/perform) the above described items.

I/We undertake, if our bid is accepted, to deliver the items in accordance with the terms and conditions contained in the bid documents, including the posting of the required performance security **within ten (10) calendar days** from receipt of the Notice of Award.

Until a formal contract/order confirmation is prepared and signed, this Bid is binding on us.

Name of Company (in print)

Signature of Company Authorized Representative

Name and Designation (in print)

Date

Annex IX

PLEASE USE THIS BID FORM. DO NOT RETYPE OR ALTER.

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

FINANCIAL BID FORM

(PRICES MUST BE INCLUSIVE OF VAT AND DELIVERED DUTIES PAID)

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

Description	Quantity	ABC (PhP)	Financial Bid (PhP)
		Total Price	Total Price
SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT	1 Lot	512,000,000.00	

TOTAL BID PRICE (Amount in Words):

____

____

Notes:

- The financial bid is inclusive of all taxes, duties, transportation costs, delivery charges and all costs relative to the project requirements including installation, testing, commissioning and training.
- The bidder shall assume all risks until the goods have been delivered at the site and accepted by DICT

BIDDER'S UNDERTAKING

I/We, the undersigned bidder, having examined the Bidding Documents including Bid Bulletins, as applicable hereby OFFER to (supply/deliver/perform) the above described items.

I/We undertake, if our bid is accepted, to deliver the items in accordance with the terms and conditions contained in the bid documents, including the posting of the required performance security **within ten (10) calendar days** from receipt of the Notice of Award.

Until a formal contract/order confirmation is prepared and signed, this Bid is binding on us.

Name of Company (in print)

Signature of Company Authorized Representative

Name and Designation (in print)

Date

Annex X

PLEASE USE THIS BID FORM. DO NOT RETYPE OR ALTER.

DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DETAILED FINANCIAL BREAKDOWN

(QUOTED PRICE MUST BE INCLUSIVE OF VAT AND DELIVERED DUTIES PAID)

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

INSTRUCTION:
-The Sum of the Detailed Financial Breakdown must be equal to the Financial Bid per Annex IX.
-Do not leave any blanks. Indicate "0" if the item is being offered for free.

ITEM	Qty	Unit Cost	Total Cost per Item
Cyber Intelligence Platform	1 Lot		
Network Protection Tools	1 Lot		
Monitoring Tools	1 Lot		
SIEM	1 Lot		
Management Tools	1 Lot		
Artificial Intelligence / Machine Learning	1 Lot		
Portable SOC	1 Lot		
Disaster Recovery Management System	1 Lot		
Storage	1 Lot		
VAPT Tools and Services	1 Lot		
Training and Services	1 Lot		
Other Equipment and Civil Works	1 Lot		
		TOTAL	

TOTAL BID PRICE (Amount in Words):

____

____

BIDDER'S UNDERTAKING

I/We, the undersigned bidder, having examined the bidding documents including Bid Bulletins, as applicable hereby OFFER to (supply/deliver/perform) the above described items.

I/We undertake, if our bid is accepted, to deliver the items in accordance with the terms and conditions contained in the bid documents, including the posting of the required performance security **within ten (10) calendar days** from receipt of the Notice of Award.

Until a formal contract/order confirmation is prepared and signed, this Bid is binding on us.

____
Name of Company (in print)

____
Signature of Company Authorized Representative

____
Name and Designation (in print)

____
Date

Annex XI-A

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

For Goods Offered From Abroad

Name of Bidder _____________________. Invitation to Bid[1] Number _______. Page
___________________________________ of ___.

1	2	3	4	5	6	7	8	9
Item	**Description**	**Country of origin**	**Qty**	**Unit price CIF port of entry (specify port) or CIP named place (specify border point or place of destination)**	**Total CIF or CIP price per item (col. 4 x 5)**	**Unit Price Delivered Duty Unpaid (DDU)**	**Unit price Delivered Duty Paid (DDP)**	**Total Price delivered DDP (col 4 x 8)**
1								
2								
3								
4								

Name of Company	Signature Over Printed Name Of Authorized Representative	Date

[1] An amount is to be inserted by the Guarantor, representing the percentage of the Contract Price specified in the Contract.

Annex XI-B

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002

For Goods Offered From Within the Philippines

Name of Bidder ______________________. Invitation to Bid[2] Number _____. Page ____________________________________ of ___.

1	2	3	4	5	6	7	8	9	10
Item	**Description**	**Country of origin**	**Qty**	**Unit price EXW per item**	**Transportation and Insurance and all other costs incidental to delivery, per item**	**Sales and other taxes payable if Contract is awarded, per item**	**Cost of Incidental Services, if applicable, per item**	**Total Price, per unit (col 5+6+7+8)**	**Total Price delivered Final Destination (col 9) x (col 4)**
1									
2									
3									
4									

Name of Company

Signature Over Printed Name
Of Authorized Representative

Date

[2]

Section IX.
Reference Documents

Annex XII

SPECIAL BANK GUARANTEE
(FOR RETENTION MONEY)

To : ___________
____
Date : ___________
____

WHEREAS, ____________________________________ with priCMSPal offices located at___________________ (hereinafter called "the Contractor/Supplier") has undertaken, in pursuance of ____________________ dated _____________ to execute supply of ________________ at _____________.

AND WHEREAS, it has been stipulated by you in the said Contract that the Contractor/Supplier shall furnish you with a Special Bank Guarantee by an authorized bank for the sum specified therein as security for compliance with their obligations in accordance to with the contract, including a warranty that the GOODS supplied are free from patent and latent defects and performance of corrective work for any manufacturing defects will be undertaken as required and that all the conditions imposed under the contract shall been fully met;

NOW THEREFORE, we hereby affirm that we are the Guarantor and responsible to you, on behalf of the Contractor, up to a total of **PhP**________________ proportions of currencies in which the Contract Price is payable, and we undertake to pay you, **upon you first written demand and without cavil or argument, any sum or sums within the limits of PhP**_______________ as aforesaid without you needing to prove or to show grounds or reasons for your demand for the sum specified therein.

We hereby further affirm that this bank guarantee is *irrevocable* and intended to answer for the performance of corrective work for any manufacturing defects, to warrant that the goods supplied are free from met by the Contractor/Supplier.

We hereby waive the necessity of your demanding that said debt from the Contractor/Supplier before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the Contract to be performed there under or of any of the Contract documents which may be made between you and the Contractor shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition or modification.

This guarantee shall be valid until ________________________________ or a minimum of one (1) year, whichever comes later.

SIGNATURE AND SEAL OF GUARANTOR

NAME OF BANK

ADDRESS

Annex XIII
Form of Performance Security (Bank Guarantee)

To : **Department of Information and Communications Technology (DICT)**
DICT Building, C.P. Garcia Avenue, Diliman, Quezon City

WHEREAS, *[insert name and address of Suppler]* (hereinafter called the "Supplier") has undertaken, in pursuance of Contract No. *[Insert number]* dated *[insert date]* to execute *[insert name of contract and brief description]* (hereinafter called the "Contract");

AND WHEREAS, it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with his obligations in accordance with the Contract;

AND WHEREAS, we have agreed to give the Supplier such a Bank Guarantee;

NOW THEREFORE, we hereby affirm that we are the Guarantor and responsible to you, on behalf of the Supplier, up to a total of *[insert amount of guarantee]*[3] proportions of currencies in which the Contract Price is payable, and we undertake to you, upon your first written demand and without cavil or argument, any sum or sums within the limits of *[insert amount of guarantee]* as aforesaid without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the Supplier before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the Contract to be performed there under or of any of the Contract documents which may be made between you and the Supplier shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition or modification.

This guarantee shall be valid until the date of your issuance of the Notice of Final Acceptance.

SIGNATURE AND SEAL OF GUARANTOR NAME OF BANK ADDRESS

[3]

Section X
Checklist of Requirements

DICT BIDS AND AWARDS COMMITTEE
CHECKLIST OF REQUIREMENTS FOR BIDDERS

Name of Company : ___________________________________

SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT
BAC4G&S-2018-002
PHP 512,000,000.00

Ref. No.	**Particulars**	
ENVELOPE 1: ELIGIBILITY AND TECHNICAL DOCUMENTS		
ELIGIBILITY DOCUMENTS		
CLASS "A" DOCUMENTS		
12.1	**(a.1.) <u>ELIGIBILITY DOCUMENTS</u>**	
	i. Registration Certificate from the Securities and Exchange Commission (SEC) for corporations, Department of Trade and Industry (DTI) for sole proprietorship, or from Cooperative Development Authority CDA) for cooperatives	
	ii. Valid and Current Business/Mayor's Permit issued by the city or municipality where the principal place of business of the prospective bidder is located OR the equivalent document for Exclusive Economic Zones or Areas; In cases of recently expired Mayor's / Business Permits, said permit shall be submitted together with the official receipt as proof that the bidder has applied for renewal with the period prescribed by the concerned local government units, provided that the renewed permit shall be submitted as a post-qualification requirement.	
	iii. Valid and Current Tax Clearance issued by Philippines' Bureau of Internal Revenue (BIR) Accounts Receivable Monitoring Division per Executive Order 398, Series of 2005;	
	iv. Copy of each of the following Audited Financial Statements for 2017 and 2016 (in comparative format or separate reports): a. Independent Auditor's Report; b. Balance Sheet (Statement of Financial Position); and c. Income Statement (Statement of Comprehensive Income)	
	<u>OR</u> **Submission of valid and current PHILGEPS Certificate of Registration and Membership (Platinum Registration) together with Annex A in lieu of (Items i., ii., iii., iv.) Eligibility Documents.** **Note:** Bidder must ensure that all Class "A" Eligibility Documents are valid and current at the time of submission of PHILGEPS Certificate of Registration and Membership (Platinum Registration). In case any of the submitted Eligibility Documents are not valid and current at the time of submission of Platinum Registration, bidders are required to submit the valid and current documents together with the Platinum Registration. In case the bidder opt to submit their Class "A" Documents, the Certificate of PhilGEPS Registration (Platinum Membership) shall remain as post-qualification requirement to be	

	submitted in accordance with Section 34.2 of the 2016 Revised IRR of RA9184. “GPPB Circular 07-2017 dated 31 July 2017”.	
	v. Statement of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid **(Annex I)**	
	vi. Statement of Completed Single Largest Contract within the last five (5) years from the date of submission and receipt of bids equivalent to at least fifty percent (50%) of the ABC **(Annex I-A).** “Similar” contract shall refer to Security Operations Center (SOC). Any of the following documents must be submitted corresponding to listed contracts per submitted Annex I-A: a. Copy of End user’s acceptance; b. Copy of Official receipt/s; or c. Copy of Sales Invoice	
	vii. Duly signed Net Financial Contracting Capacity Computation (NFCC)* per **Annex II,** in accordance with ITB Clause 5.5 or a committed Line of Credit equivalent to at least ten percent (10%) of the ABC from a universal or commercial bank a. Should the bidder opt to submit NFCC, computation must be equal to the ABC of the project. *NFCC = [(Current Assets minus Current Liabilities) (15)] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started coinciding with the contract to be bid. **Notes:** A. The values of the bidder’s current assets and current liabilities shall be based on the data submitted to BIR through its Electronic Filing and Payment System. B. Value of all outstanding or uncompleted contracts refers those listed in Annex-I. C. The detailed computation using the required formula must be shown as provided above. D. The NFCC computation must at least be equal to the total ABC of the project. **OR** b. Should the bidder opt to submit a Committed Line of Credit, it must be at least equal to ten percent (10%) of the ABC issued by a Local Universal or Local Commercial Bank.	
CLASS “B” DOCUMENTS (FOR JOINT VENTURE)		
	viii. For Joint Ventures, Bidders to submit either: 1. Copy of the JOINT VENTURE AGREEMENT (JVA) in case the joint venture is already in existence; or 2. Copy of Protocol / Undertaking of Agreement to Enter into Joint Venture signed by all the potential join venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful. **(Annex III)** **The JVA or the Protocol/Undertaking of Agreement to Enter into Joint Venture (Annex III) must include/specify the company/partner and the**	

name of the office designated as authorized representative of the Joint Venture.

For Joint Venture, the following documents must likewise be submitted by each partner:

1. Registration Certificate from the Securities and Exchange Commission (SEC) for corporations or from Department of Trade and Industry (DTI) for sole proprietorship, or from Cooperative Development Authority (CDA) for cooperatives;

2. Valid and Current Business/Mayor's Permit issued by the city or municipality where the principal place of business of the prospective bidder is located OR the equivalent document for Exclusive Economic Zones or Areas;

   In cases of recently expired Mayor's / Business Permits, said permit shall be submitted together with the official receipt as proof that the bidder has applied for renewal with the period prescribed by the concerned local government units, provided that the renewed permit shall be submitted as a post-qualification requirement;

3. Valid and current Tax Clearance issued by Philippines' Bureau of Internal Revenue (BIR) Accounts Receivable Monitoring Division per Executive Order 398, Series of 2005;

4. Copy of each of the following Audited Financial Statements for 2016 and 2015 (in comparative form or separate reports):
   a. Independent Auditor's Report;
   b. Balance Sheet (Statement of Financial Position); and
   c. Income Statement (Statement of Comprehensive Income)

   Each of the above statements must have stamped "received" by the Bureau of Internal Revenue (BIR) or its duly accredited and authorized institutions.

OR

5. Submission of valid and current PHILGEPS Certificate of Registration and Membership (Platinum Registration) together with Annex A in lieu of the eligibility documents.

   Note: Bidder must ensure that all Class "A" Eligibility Documents are valid and current at the time of submission of PHILGEPS Certificate of Registration and Membership (Platinum Registration). In case any of the submitted Eligibility are not valid and current at the time of submission of Platinum Registration, bidders are required to submit the valid and current documents.

   In case the JV Partners opt to submit their Class "A" Documents, the Certificate of PhilGEPS Registration (Platinum Membership) shall remain as post-qualification requirement to be submitted in accordance with Section 34.2 of the 2016 Revised IRR of RA9184. "GPPB Circular 07-2017 dated 31 July 2017".

For item (v) to (vi) of the required Eligibility Documents, submission by any of the Joint Venture **partner constitutes compliance.**

<table>
<tr><th colspan="3">TECHNICAL DOCUMENTS</th></tr>
<tr><td>12.1 (b)(i)</td><td>Bid security shall be issued in favor of the <b>DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT) valid at least one hundred twenty (120) days after date of bid opening</b> in any of the following forms:
a) BID SECURING DECLARATION per <b>Annex IV;</b> or
b) Cashier's / Manager's Check equivalent to at least 2% of ABC issued by an Universal or Commercial Bank.
c) Bank Draft / Guarantee or Irrevocable Letter of Credit issued by a Universal or Commercial Bank equivalent to at least 2% of the ABC: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank
d) Surety Bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security equivalent to at least 5% of the ABC
<table>
<tr><th colspan="2">Description</th><th>SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT</th></tr>
<tr><td colspan="2"><b>Qty</b></td><td>1 Lot</td></tr>
<tr><td colspan="2"><b>Total ABC (PhP)
(VAT Inclusive)</b></td><td>PhP512,000,000.00</td></tr>
<tr><td rowspan="4"><b>BID SECURITY</b></td><td><b>Cashier's / Manager's Check equivalent to at least 2% of the ABC (PhP)</b></td><td rowspan="2">PhP10,240,000.00</td></tr>
<tr><td><b>Bank Draft / Guarantee or Irrevocable Letter of Credit equivalent to at least 2 % of the ABC (PhP)</b></td></tr>
<tr><td><b>Surety Bond equivalent to at least 5% of the ABC (PhP)</b></td><td>PhP25,600,000.00</td></tr>
<tr><td><b>Bid Securing Declaration</b></td><td>No required percentage</td></tr>
</table>
</td><td></td></tr>
<tr><td>12.1 (b)(ii)</td><td>Proof of Authority of the Bidder's authorized representative/s:
a) FOR SOLE PROPRIETORSHIP (IF OWNER OPTS TO APPOINT A REPRESENTATIVE): Duly notarized Special Power of Attorney
b) FOR CORPORATIONS, COOPERATIVE OR THE MEMBERS OF THE JOINT VENTURE: Duly notarized Secretary's Certificate evidencing the authority of the designated representative/s.
c) IN THE CASE OF UNINCORPORATED JOINT VENTURE: Each member shall submit a separate Special Power of Attorney and/or Secretary's Certificate evidencing the authority of the designated representative/s.</td><td></td></tr>
<tr><td rowspan="10">12.1 (b)(iii)</td><td>Omnibus Sworn Statements using the form prescribed. <b>(Annex V)</b></td><td></td></tr>
<tr><td>a) Authority of the designated representative</td><td></td></tr>
<tr><td>b) Non-inclusion of blacklist or under suspension status</td><td></td></tr>
<tr><td>c) Authenticity of Submitted Documents</td><td></td></tr>
<tr><td>d) Authority to validate Submitted Documents</td><td></td></tr>
<tr><td>e) Disclosure of Relations</td><td></td></tr>
<tr><td>f) Compliance with existing labor laws and standards</td><td></td></tr>
<tr><td>g) Bidder's Responsibility</td><td></td></tr>
<tr><td>h) Did not pay any form of consideration</td><td></td></tr>
<tr><td>i) Company Official Contact Reference</td><td></td></tr>
<tr><td>12.1 (b)(iv)</td><td>Company Profile <b>(Annex VI).</b> Company printed brochure may be included</td><td></td></tr>
<tr><td>12.1 (b)(v)</td><td>Vicinity / Location of Bidder's principal place of business</td><td></td></tr>
</table>

12.1 (b)(vi)	Certificate of Performance Evaluation **(Annex VII)** showing a rating at least Satisfactory issued by the Bidder's Single Largest Completed Contract Client stated in the submitted Annex I-A;	
12.1 (b)(vii)	Completed and signed Technical Bid Form **(Annex VIII)**	
12.1 (b)(viii)	Business Registration Certificate (BRC) with a minimum of five (5) years of experience in the field of intelligence, threat detection and cyber security	
12.1 (b)(ix)	Valid Certification from at least two (2) of the bidder's clients to prove that they have performed cyber forensic investigations specifically involving external attackers	
12.1 (b)(x)	Bidder's portfolio or any documentary report to prove that they have deep intelligence in cyber threat actors especially those related to financial crimes and critical infrastructure	
12.1 (b)(xi)	Product specification and/or datasheet to prove that it has the technology to scale the forensic assessment to all Windows systems;	
12.1 (b)(xii)	Product datasheet to prove expertise in the following: a) Analysis of computer systems, network traffic transiting between customer's network and the Internet b) Assessment of regular status report, assessment report of relevant findings, and recommendations for improvement and executive brief report c) Executive-level briefing detailing necessary recommendations to improve incident preparedness capabilities d) Computer security incident response support e) Forensics, log and advanced malware analysis f) Advanced threat actor response support g) Advanced threat/incident remediation assistance	
12.1 (b)(xiii)	Technical Data Sheet or equivalent document for the following tools and services: a) Threat Intelligence Platform b) Web Intelligence Tool c) Network Protection Tools d) Next Generation Firewall (NGFW) e) Distributed Denial of Service (DDos) Protection Tool f) IPS/IDS g) Application Delivery Controller (ADC) h) Log Collection and Correlation Tool i) Artificial Intelligence (AI) / Machine Learning j) Portable CMS k) Disaster Recovery Management System Tool l) VAPT Tool	
12.1 (b) (xiv)	Valid and Current Certificate of Distributorship / Dealership/ Resellership of the following product being offered, issued by the principal or manufacturer of the product (if Bidder is not the manufacturer). If not issued by manufacturer, must also submit certification / document linking bidder to the manufacturer. a) Web Intelligence Tool b) Network Protection Tools c) Next Generation Firewall (NGFW) d) Distributed Denial of Service (DDos) Protection Tool e) IPS/IDS f) Application Delivery Controller (ADC) g) Log Collection and Correlation Tool h) Artificial Intelligence (AI) / Machine Learning i) Portable CMS j) Disaster Recovery Management System Tool k) VAPT Tool	

<table>
<tr><td>12.1 (b)(xv)</td><td>Compliance with the Schedule of Requirements as per Section VI</td><td></td></tr>
<tr><td>12.1 (b) (xvi)</td><td>Compliance with the Technical Specifications as per Section VII</td><td></td></tr>
<tr><td colspan="3"><b>ENVELOPE 2: FINANCIAL DOCUMENTS</b></td></tr>
<tr><td>13.1 (a)</td><td>Completed and signed Financial Bid Form. Bidder must use, accomplish and submit Financial Bid Form hereto attached <b>Annex IX.</b>
<table>
<tr><th rowspan="2">Description</th><th rowspan="2">Qty</th><th>ABC ₱ (VAT Inclusive)</th></tr>
<tr><th>Total</th></tr>
<tr><td>SUPPLY, INSTALLATION AND DELIVERY OF CYBERSECURITY MANAGEMENT SYSTEM PROJECT</td><td>1 Lot</td><td>PhP512,000,000.00</td></tr>
</table>
The ABC is inclusive of VAT. Any proposal with a financial component exceeding the ABC shall not be accepted. Further, the sum of bid for each item indicated in the <b>Detailed Financial Breakdown per Annex X</b> must be equal to the signed and submitted Financial Bid Form per Annex VII.</td><td></td></tr>
<tr><td>13.1 (a)</td><td><b>Detailed Financial Breakdown per Annex X</b></td><td></td></tr>
<tr><td>15.4(a) (i) & 15.4(b) (ii)</td><td>Completed <b>“For Goods Offered from Abroad”</b> and/or <b>“For Goods Offered From Within the Philippine”</b> Forms per <b>Annex XI-A</b> and <b>Annex XI-B, whichever is applicable.</b></td><td></td></tr>
<tr><td>13.1 (b)</td><td>If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a Certification from the DTI, SEC or CDA to be enclosed pursuant to the Revised IRR of R.A. 9184.</td><td></td></tr>
<tr><td><b>NOTE:</b></td><td><b>In case of inconsistency between the Checklist of Requirements for Bidders and the provisions in the Instruction to Bidders/Bid Data Sheet, the Instruction to Bidders/Bid Data Sheet shall prevail</b></td><td></td></tr>
</table>